IT Security Products for Corporate Users

Review of IT Security Suites for Corporate Users, 2009

Language: English
May 2009
Last revision date: 2009-05-27

www.av-comparatives.org

Table of Contents

The risk of malicious software 3
Management Summary 5
SPAM-Test 9
HIPS-Test 11
Product Review Section 13
AVIRA 14
ESET 29
G DATA 42
Kaspersky 54
SOPHOS 72
Symantec 85
TrustPort 97

Appendix A – Feature list & System Requirements

The risk of malicious software

Most organizations are aware of the risk threatening their IT environment. Viruses, Trojans, Worms, Exploits and many others threats represent a serious risk for the IT department. A collapse of the IT systems could mean grave financial losses right up to insolvency for a company.

The IT departments of companies are conscious about this problem. Getting the best protection against this threat is the only issue. An Anti-Virus safeguard alone is far too inadequate. There are too many threats starting from contaminated e-mails, exploits etc. What is required is comprehensive protection suite against all of these.

Functional Diversity

Because of the immense functional diversity of various Anti-Virus suites and corporate products, it is becoming increasingly difficult for decision-makers in the IT sector to get a proper overview. Which product should one opt for and for which area of application?

During these tests our main focus has not been on detection rates but, instead, on the products with respect to their handling and user-friendliness and the scope of functionality. We have compiled the functional scope of various products in an extensively detailed table.

For detection rates of individual products please refer to our website
http://www.av-comparatives.org under the tab “Main Tests”

Target Group

This report is primarily targeted at IT Administrators in organizations of all sizes. In order to present an overview, we have depicted the installation procedure in detail. Administrators can in future comprehend from this how one handles the program subsequently. This represents merely the status at present, since software products are constantly subject to ongoing development and are updated continuously.

Hardware and Software

Organizations seldom use the latest hardware available in the market. Based on a survey conducted on 50 organizations of various sizes, which we have carried out in the run-up to the tests, the hardware that we have used is equivalent to the generation of computers generally deployed.

The selection intentionally included the somewhat older configurations in order to reflect the real status of the IT environment in various organizations.

Server Configuration

CPU:	Dual Xeon
RAM:	4 GB RAM
Hard disk:	250 GB, S-ATA
OS:	Windows 2003 Small Business Server incl. Service Packs and Security Updates until 28th February 2009
Server Role:	Domain controller including Exchange 2003. DNS including Forwarders.

Client Configuration

CPU:	Intel Pentium IV, 3 GHz
RAM:	1 GB RAM
Hard disk:	40 GB, S-ATA
OS:	Windows XP Professional SP3, Security Updates until 28th February 2009

Management Summary

All the participants have done their homework. We can anticipate one thing: Our test demonstrates that the manufacturers are very responsive to the needs within an organization. There are no exceptions and all products comply with the prevalent security standards. Any purchase decision must be made depending on the specific area of application in the future and special attention must be paid to the functional scope of the products.

Certain products are more suitable for enterprises, i.e. the large and largest of organizations and certain other products are more suitable for small and medium-scale business operations while others satisfy the needs of small users.

To sum it up, the products of Symantec, Kaspersky and G DATA became popular as very good all-round products and AVIRA became a good choice for medium-scale business establishments. SOPHOS reflected its strength and experience as a purely corporate product by means of a perfect Active Directory implementation. The corporate solution provided by ESET has caught our attention particularly as a consequence of its large potential for the enterprise market. We consider Trustport to be an ideal candidate in the area of small business establishments.

SYMANTEC have undoubtedly established their enormous experience in the software security industry. This suite left nothing more to be desired. It was merely the somewhat long time required for installation, especially the creation of the database, and the elementary database support that called for improvement.

The strength of G DATA lies in the simplicity of its installation procedure. The suite was the easiest software to install. What needs to be highlighted is also the server distribution of the master-slave configuration and the exemplary solution for providing the failover functionality.

Indisputably, ESET offers the largest number of configuration options. The package supports the largest number of deployment methods. However, thorough preparation is in any case mandatory to the extent outlined above. For installations of 50,000 users and above, you simply cannot ignore this suite.

Even the software from KASPERSKY is a fully developed suite, which has great strengths especially when it comes to database support. The suite was one of the few products that supported MY SQL. Even the function of logging in, which is very important in many organizations, has been implemented very well by KASPERSKY.

The management console of AVIRA, which is designed with a simple structure, is ideal for small and medium-scale business operations. It is really simple and comfortable for the administrator to distribute the software to the clients. The administrator console is clearly laid out in the case of small to medium-scale business operations, but it becomes cumbersome and unwieldy when there are many thousands of clients.

SOPHOS demonstrates that it lays its focus on organizations, with the Active Directory support that it provides. It has, undoubtedly, the best implementation for Active Directory support. As a result of this support, it is possible to transfer different roles to various

persons for the administration of the antivirus system in high-security environments, thus relieving the administrator.

The subject of "Usability and Management" needs to be highlighted with the product of TRUSTPORT. In this case, it is really simple to navigate through the console without having to study the user manual and, thus, find the various functions and actions quickly and easily. This aspect has been implemented excellently by TRUSTPORT and navigating through various management consoles leaves nothing to be desired.

Status

What we have noted with almost all the products tested is the unpretentious implementation of the real-time status. It is important for the user, especially in corporate establishments, to know what the Anti-Virus system is doing at any given point of time. Thus, any possible debugging can be made considerably simpler if the user can supervise the various modules comfortably and is constantly aware of the status. What has already become a standard feature in the case of firewalls is, by and large, omitted in the products tested here.

All in all, one can say that the user should not only take the price into consideration when selecting the Anti-Virus product, since most of them are comparable in this respect, with even the virus detection rates being very similar (these can be referred to on our website in the tests conducted by us in February), but, on the contrary, he should first concentrate on the functions that he really requires. These include simple handling, ease of installation, sorting options for individual clients in large organizations, the feature of defining multiple servers as fail-over servers, etc. The appendix contains a detailed overview of these features.

Improvement of the Products

Our findings during the review were welcome by the vendors. Some of the improvements we suggested in this report will be considered and implemented in the next releases of the products.

We are happy to report that all products reviewed in this report received the AV-Comparatives Seal of Approval. All products performed their primary functions very well, as can be expected from established business Anti-Virus products. IT Administrators may find that some products fit their business needs better than others because they address a specific set of features they are looking for.

Overview

We try to give an overview of the products, it can be used as a help for doing your decision. Please try the products on your own system before making a purchase decision based on this review. All vendors offer trial-versions of their products and have qualified resellers in the most countries. The review and the below table contains our subjective appraisal we got during the test-period and the publicly available information on the vendors websites.

	AVIRA	ESET	G DATA	Kaspersky	Sophos	Symantec	TrustPort
Installation on the Server	****	***	*****	*****	*****	*****	***
Deployment at the Client	****	****	****	****	*****	*****	***
Usability and Management	***	***	*****	*****	*****	*****	***
Performance	*****	*****	*****	*****	****	*****	****
Target Audience							
SOHO Business	*****	**	*****	*****	****	*****	****
Small Business	*****	****	*****	*****	****	*****	***
Medium Business	****	*****	*****	*****	*****	*****	***
Enterprise	***	*****	****	****	****	*****	**
User Manual	****	***	****	****	****	****	***
MS AD Support	*	****	****	****	*****	****	
Database Support	**	***	****	*****	****	****	*
Ease of Installation	*****	**	*****	****	*****	*****	***
Logging	***	**	***	****	****	***	**
Real-Time Status	****	***	***	****	****	***	****
SPAM	***	*****	*****	****	*****	*****	***
Technical Support	****	*****	****	*****	*****	*****	****
Website	*****	*****	****	*****	****	*****	****
Overall Assessment	****	****	*****	*****	*****	*****	****

Tested Products

The following vendors participated in the conducted review and tests:

AVIRA	**www.avira.com**
ESET	**www.eset.com**
G DATA	**www.gdata.de**
Kaspersky	**www.kaspersky.com**
Sophos	**www.sophos.com**
Symantec	**www.symantec.com**
TrustPort	**www.trustport.com**

All images are copyright
of the respective vendor.

SPAM-Test

Spam is a very annoying issue, which can borrow much work time and therefore cost money. Due that, efficient spam filters are required. On the other hand, spam filters must not filter out any wanted mails (ham), as this could be dangerous in business-life.

The mails were filtered directly on the Exchange Server. If there was no Exchange-Plug-In by the product, it was filtered on the client. We used Outlook 2003 (with disabled Junk-Mail-Filter for testing purposes).

All settings of the tested products were left on DEFAULT WITHOUT TRAINING. By training the spam filters the filtering rates could be increased further.

SPAM-Test

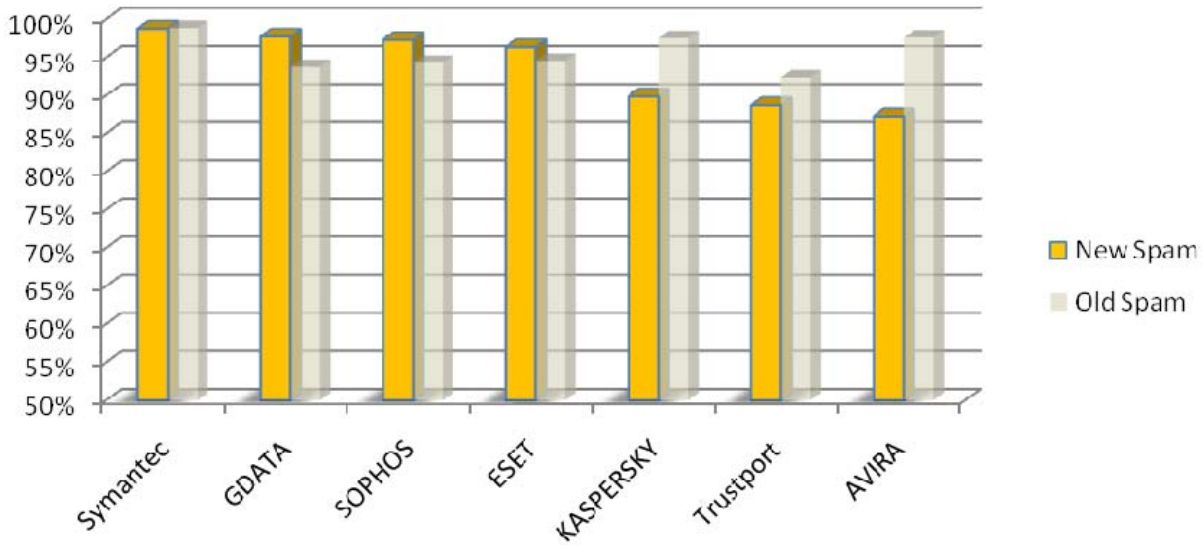
We tested the spam filter of the products in two ways:

1. For the first test, we took only SPAM-mails which have been collected continuously and were not older than 3 weeks (about 10000 E-Mails). That's the meaningful test.
2. We took randomly selected about 4000 SPAM-mails, which were 1 to 3 months old.

HAM-Test

We tested on about 5000 wanted mails, which have been collected continuously and were not older than 3 weeks.

SPAM-Test Results



	New Spam	(Old Spam)
Symantec	**99%**	(99%)
G DATA	**98%**	(94%)
Sophos	**97%**	(94%)
ESET	**96%**	(95%)
Kaspersky	**90%**	(98%)
Trustport	**89%**	(92%)
AVIRA	**87%**	(98%)

Percentages (rounded) are Spam Filtering Rates.

HAM-Test Results

Very positive is the fact, that **none** of the tested products **classified any wanted mail** (Ham-Mail) **as SPAM.**

The spam filters can be set on different levels, you have to find the best selection for your own. Also Whitelisting and Blacklisting is an opportunity.

HIPS-Test

Many products have nowadays Host Intrusion Prevention Systems (HIPS), behavior-blocking and other mechanism to protect against malware and other harmful system changes.

This HIPS-Test considers all the various protection and detection features of the product, not just the HIPS-Part.

We did the test simulating a normal user, with real world conditions. We surfed the internet on relatively new sites that were hosting malicious software. We tested with 25 randomly selected websites, containing different malware-types including Rogue-Software, Password-Stealers, Bots, Spyware, Adware, Trojans, etc.

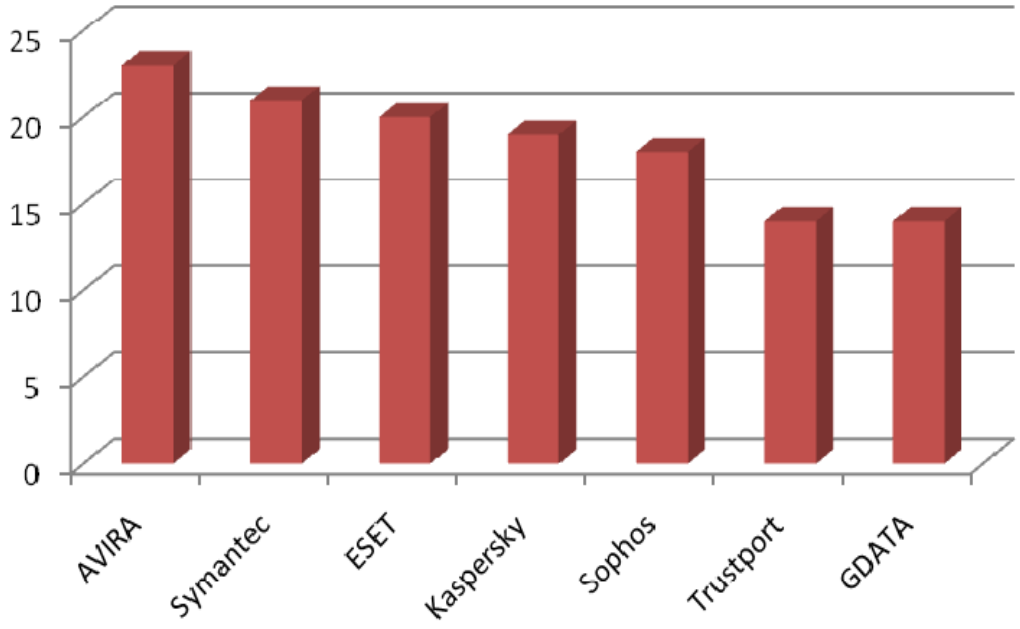
All products were up to date and the websites were surfed on at the same time. If the administrator would change the settings, enabling all protection features and higher settings, a higher protection could be achieved.

Detection-Level

Most products blocked the threats already during the download attempt. Some few more were discovered during the installation.

Some products do not have HIPS etc. activated by default and do not run with high heuristics on the clients by default (e.g. to avoid false alerts and performance-loss). Due that, it is highly recommended to perform regularly On-Demand scans with highest settings.

HIPS-Test Results



Product	Protected against
AVIRA	23 of 25
Symantec	21 of 25
ESET	20 of 25
Kaspersky	19 of 25
Sophos	18 of 25
Trustport	14 of 25
GDATA	14 of 25

Product Review Section

The products are in alphabetical order.

AVIRA

Test Software:

AVIRA Antivir Server (Windows) Version 9	→	File Server Protection
AVIRA Antivir Exchange 2000/2003	→	Exchange Server Mail Protection
AVIRA Antivir Security Management Center	→	Centralized Control Console and Deployment
AVIRA AntiVir Professional, Version 9	→	Client Virus Protection

Installation Procedure

Downloading the Products:

Menu navigation provided by the manufacturer has been structured coherently and kept simple. It is easy for the user to find the desired products and it is possible to download all products with their entire scope of functionality even without registration.

Especially for small and medium business up to 100 clients there is a separate product package called Avira SmallBusiness Suite that likewise consists of the products Avira Security Management Center, Avira AntiVir Server, Avira AntiVir Professional and Avira AntiVir Exchange. What´s special about this package is that it comes with a configuration wizard that makes it very easy to setup the security environment and roll out the products

Registration is required for a test key. Thereafter, 30 days are available to test the desired products extensively. Data is then forwarded to a certified partner of AVIRA.

Using a broadband connection, the time taken to download was as follows:

AVIRA Antivir Server (Windows) Version 9 (28.9 MB) ⟹ 22 seconds

AVIRA Antivir Exchange 2000/2003 (107 MB) ⟹ 01:23 min.

AVIRA Antivir Security Management Center (58.2 MB) ⟹ 44 seconds

AVIRA AntiVir Professional, Version 9 (to be used in the AVIRA SMC or in case of non-availability of Internet connection) (30.2 MB) ⟹ 25 seconds

Installing the Products:

From this point onwards, one should refer to the manual since considerable time can be saved by following the correct sequence when installing the products.

The first step should be to begin with the AVIRA SMC (Security Management Center).

The SMC installation package consists of a ZIP archive on the computer. This ZIP archive consists of 4 components.

AntiVir_Security_Management_Center_Agent_de.exe

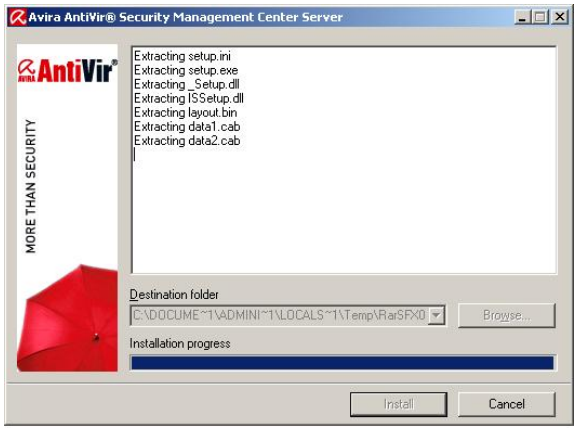
AntiVir_Security_Management_Center_Frontend_de.exe

AntiVir_Security_Management_Center_Server_de.exe

AntiVir_Security_Management_Center_UNIX_Agent.tgz

Barring the UNIX agent, it would have been desirable to have an installer, which could be used to select all 3 components,

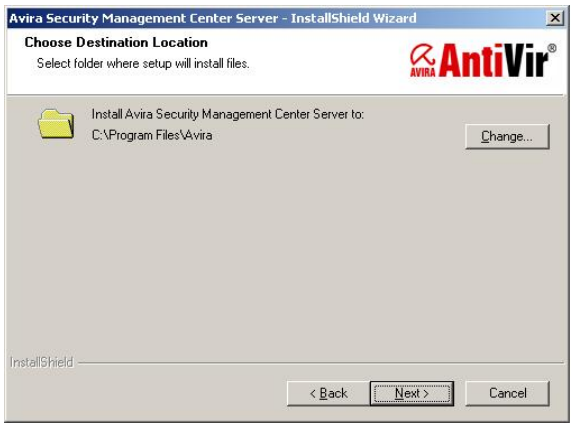
We begin – as enumerated in the manual - with the installation of the SMC server:



The setup assistant displays the welcome window after extracting the installation files in a temporary folder.

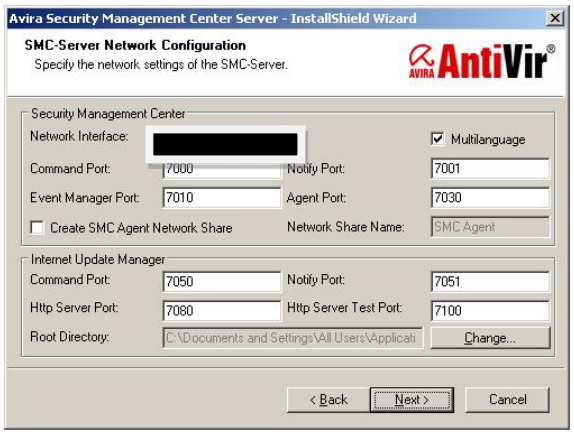
We accept the mandatory terms of the license agreement:

Thereafter, we can select the destination for the SMC files:



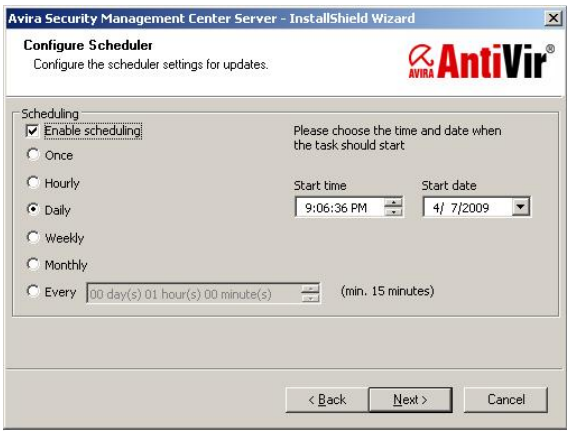
Here, we specify the ports, which should open the server process so that the communication with individual components can be ensured.

Using the option "Create SMC Agent Network Share" one can create a shared folder where the agent installation files are saved. This Share folder is used for the unattended installation of the agent using a login script.

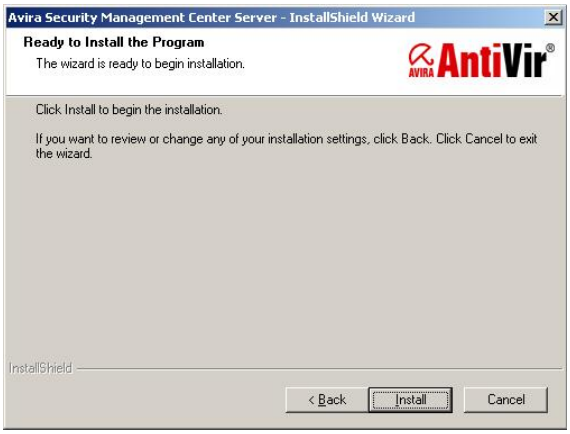


The SMC Front-end user can be defined here. The SMC offers the option of an AD account on the server as a user account or its own user, which is saved in the user administration of the SMC.

This menu is used to configure the settings for the SMC update. It is, however, not apparent whether the updates pertain to the SMC program components or to the virus patterns. In my opinion, the daily option for updating the virus patterns is not adequate in order to react in time to new virus threats.

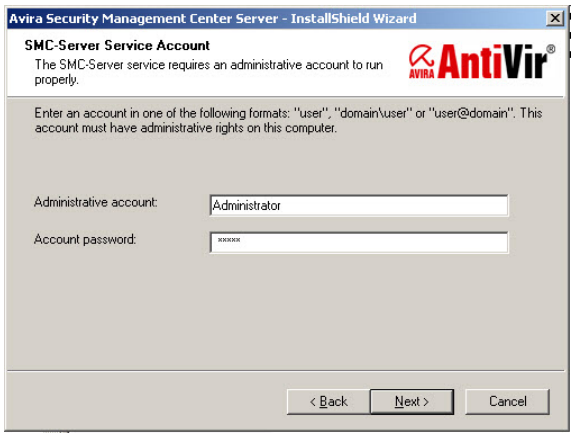


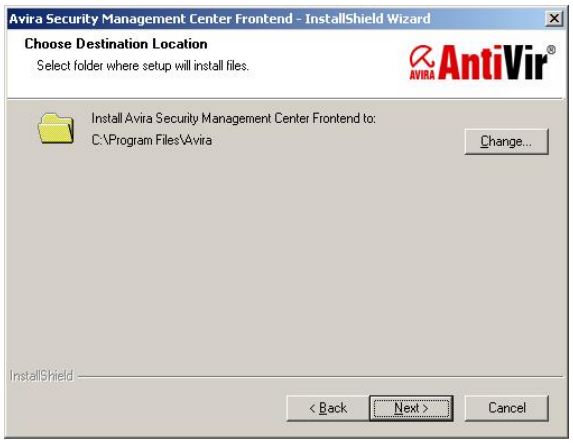
A final confirmation is required before the SMC server center is installed.

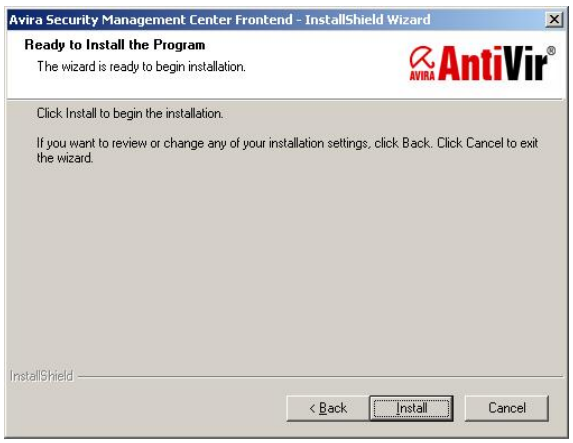


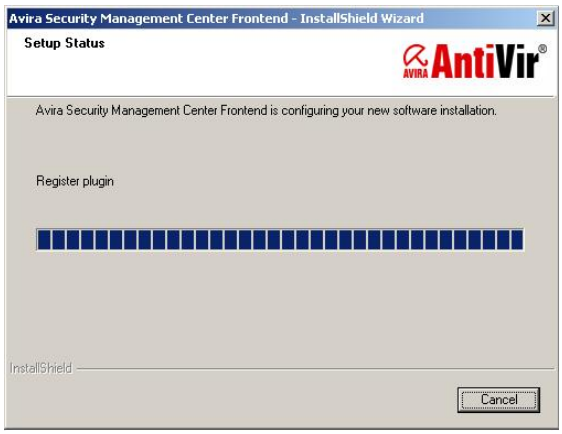
After completing the installation, we can begin with the next step, which is the SMC front-end.

The installation of the SMC-Server requires an administrative account which must be entered in the following dialogue:



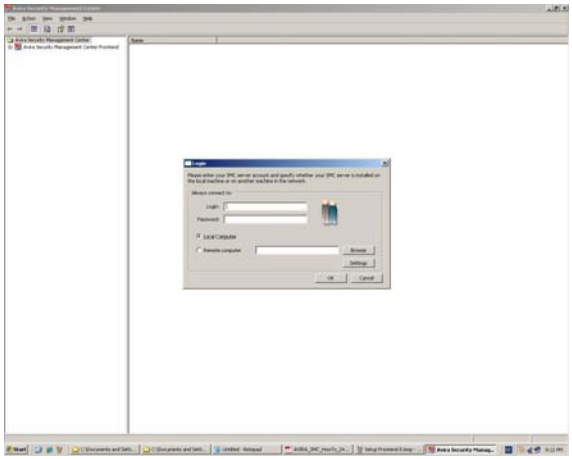




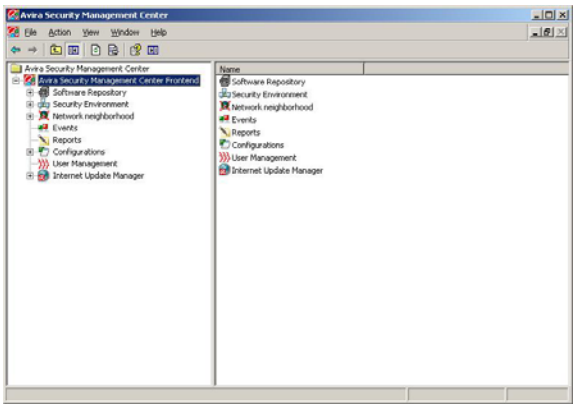


Configuring the SMC:

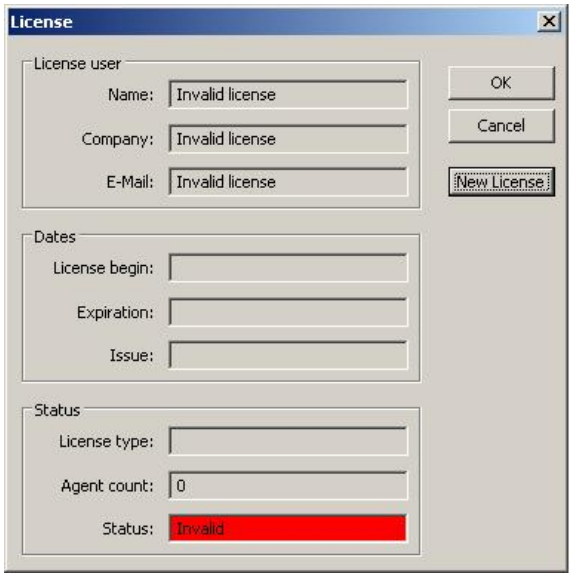
After completing the installation of the front-end, we can start the SMC console and login with the user names defined at the time of installing the server:



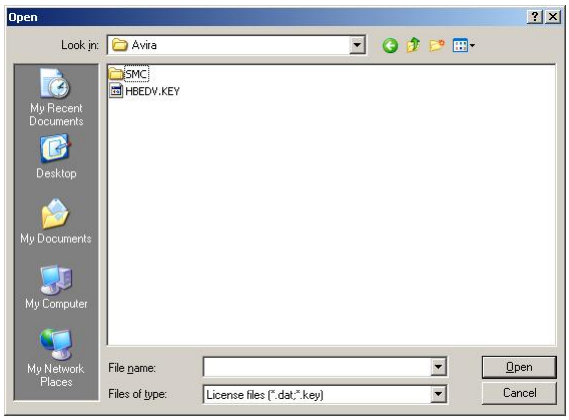
The SMC console is displayed after logging in successfully:



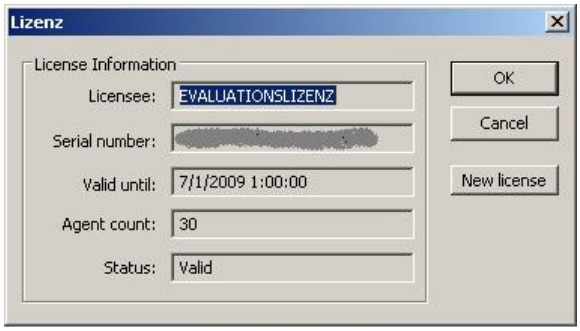
As the first step, we must now link up the licenses for the SMC. To do this, we must click with the right mouse button on the option "AVIRA Security Management Center Front-end" and select the option "Licenses":



We select the license file saved locally in order to integrate the licenses for our products:

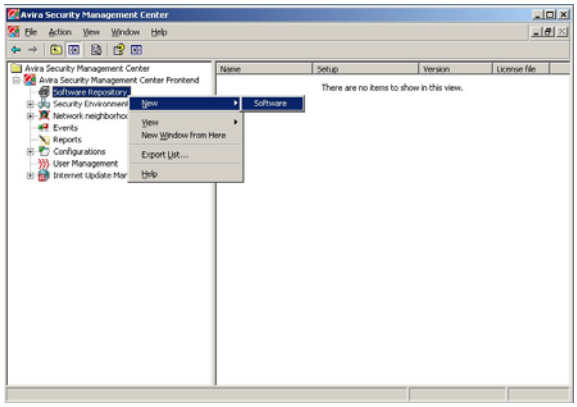


After selecting the license file, we can see whether the license is active and has been incorporated correctly:

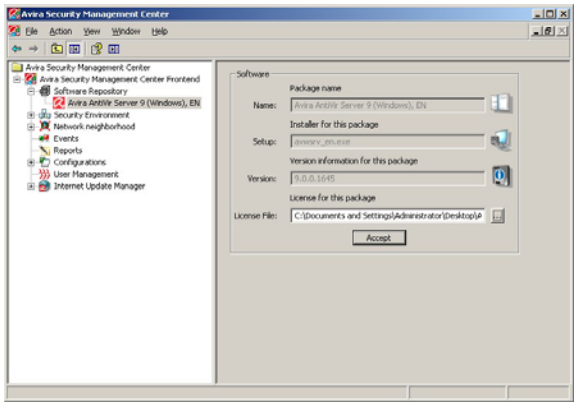


At this stage, we will integrate those software packages, including the licenses, which we want to distribute across the Clients, in the SMC.

To do this, we navigate to the Software Repository and select the option "New" => "Software" in the pop-up menu.



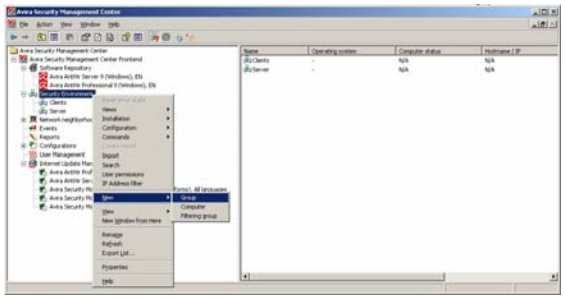
After selecting the software package, we must also copy the associated license, which is done in the same menu:



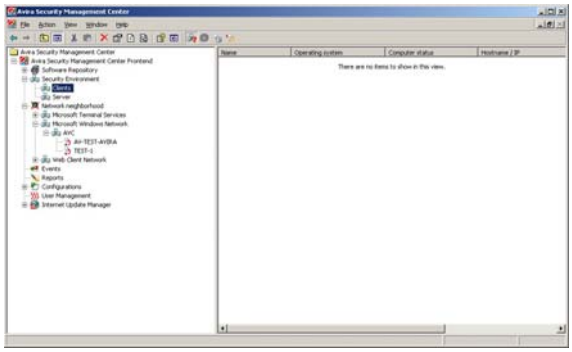
After clicking on the "Accept" button, the license is checked for validity.

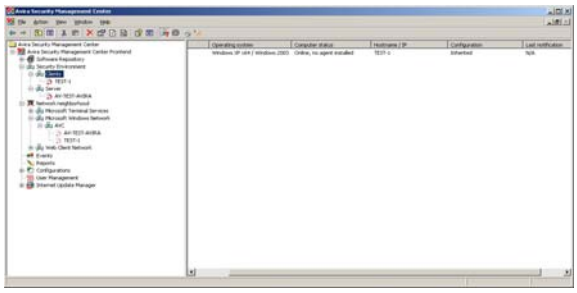
After incorporating the software packages successfully for distributing the software on the Clients, we need to integrate the Clients themselves in the SMC.

For this purpose, we must first define the so-called "Security Groups". This option permits the selection of various configuration and organizational criteria. In our case, we shall create 2 groups having the names "Server" and "Clients". To create these groups, we shall select the option "New" => "Group" in the pop-up menu of the "Security Environment" option.

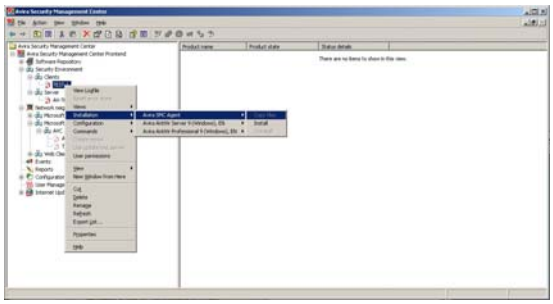


To incorporate the Clients in the groups, we merely need to navigate to the "Network Neighborhood" accounts and drag and drop the desired Clients in the relevant group. There is also an import feature that allows importing clients using a CSV file or importing clients directly from an active directory. Just right click on the security environment and choose <import>. If importing from an AD there are various options, e.g. to ignore the AD hierarchy or create groups based on the DNS names or organizational units.

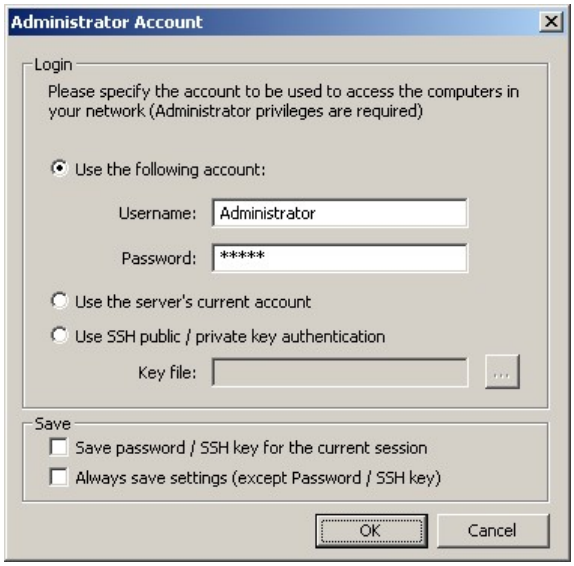




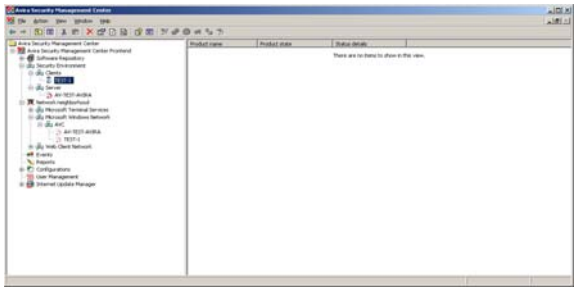
In the next step, the individual products of AVIRA are installed on the Clients and the Server. For this purpose, we simply go to the desired Client and select "Installation" and then "AVIRA SMC Agent" using the right mouse button, in order to install the SMC Agent on the computer, so that the Client always sends the latest status updates to the SMC console and it is possible to install the software via the SMC.



In the next step, we specify the user for whom the push installation needs to be done.

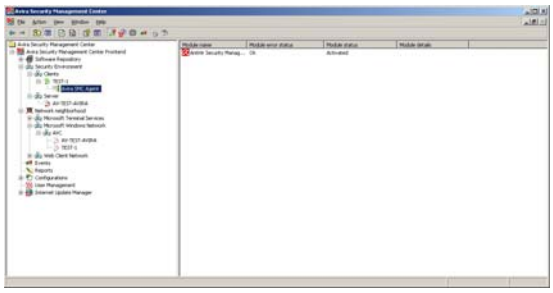


Here too, the good thing is that there are various options for the authentication procedures.



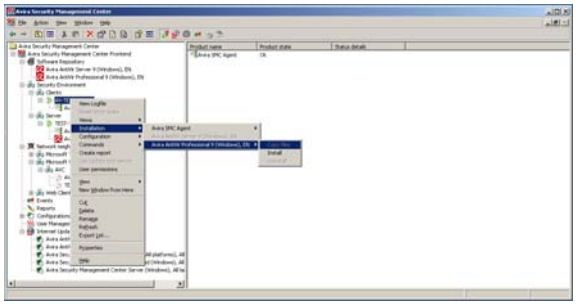
During installation, a sandglass is displayed until the SMC console receives con-

firmation about the completion of the installation on the Client.

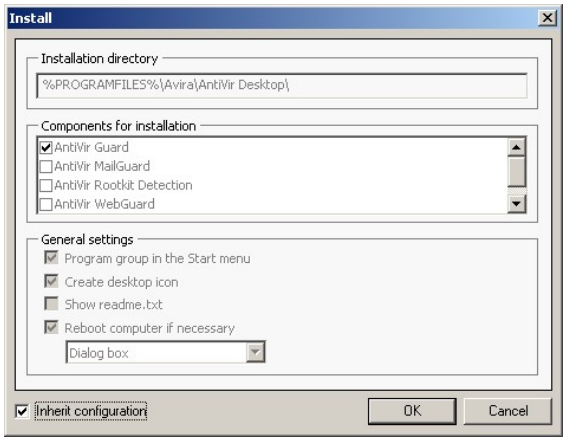


After the installation has been completed successfully, the product installed is displayed below the Client.

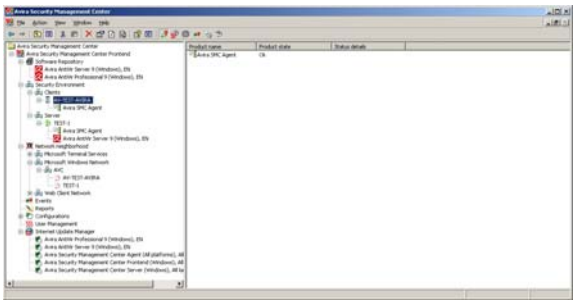
It is now time to install the antivirus Client.



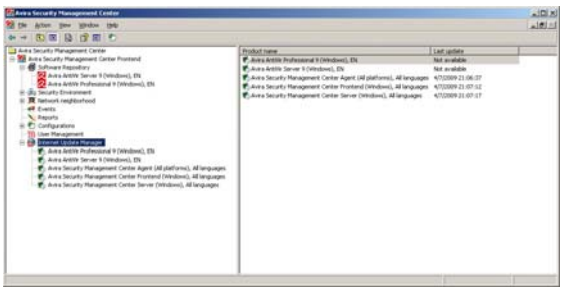
In this step, we can choose the components and the settings of the AVIRA Client to be installed on the selected system.



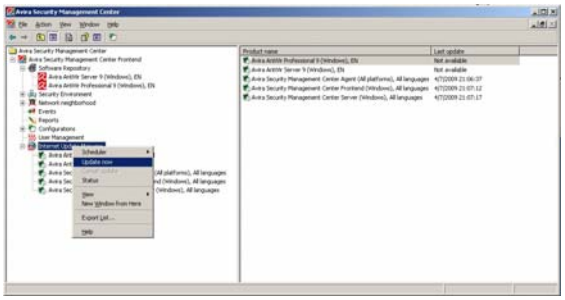
After successful installation, the product is displayed below the system.



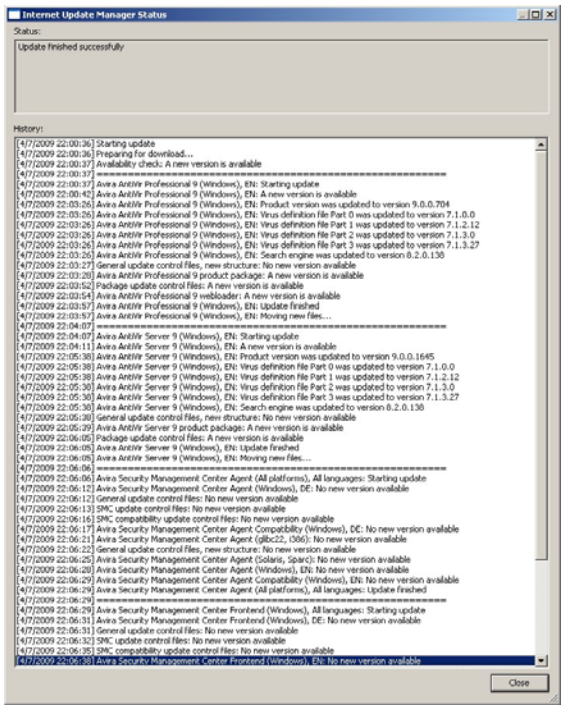
After installing the products on the Clients successfully, we can configure the updates.

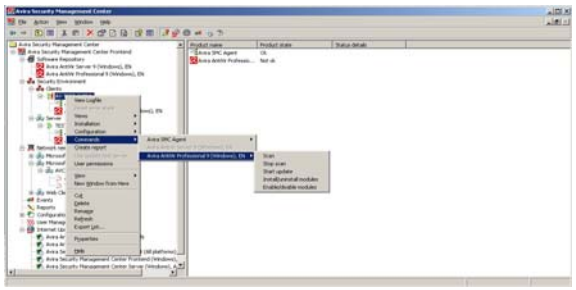


For this purpose, we select the desired product and the option “Update” in the drop-down menu.

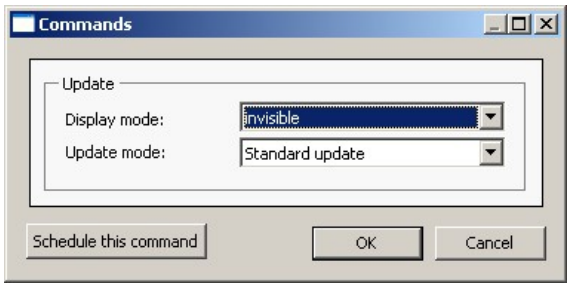


After performing the update of the software products successfully, we can also initiate a manual update on the Clients.





The console also asks for the update method to be used:



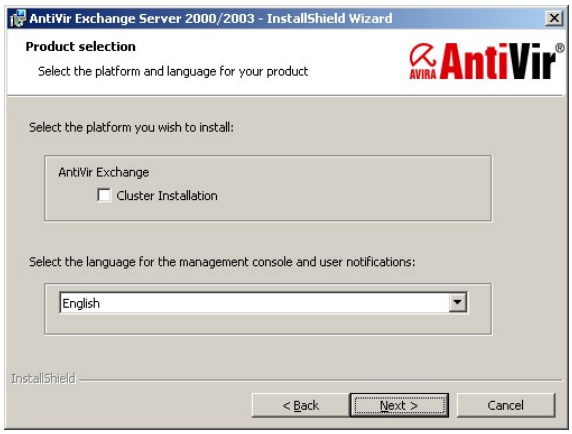
In this case, we choose an update method that is invisible to the user and runs in the background. You can choose between "Standard Update" and "Product Update" for the update method. With "Standard Update", both pattern updates and product updates are carried out. With "Product Update" product, engine and pattern updates are implemented.

An attractive feature here is that everything for the systems can be selected with the help of pop-up menus. You can configure everything via the SMC comfortably, starting from the update intervals right up to the scanner settings.

User navigation has been designed well and in a friendly manner and you rarely need to refer to the manual, since everything has been explained clearly and is easy to understand. Navigation is a simple task as a result of the MMC structure of the SMC console.

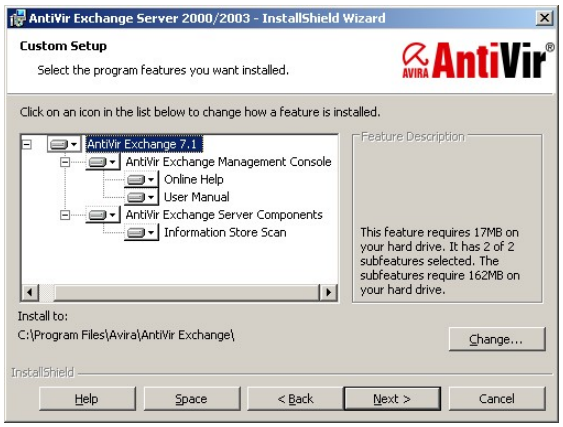
We shall now install the product, "AVIRA Antivir for Exchange Server", on our SBS.

Here too, the user-friendly wizard guides you through the installation procedure:

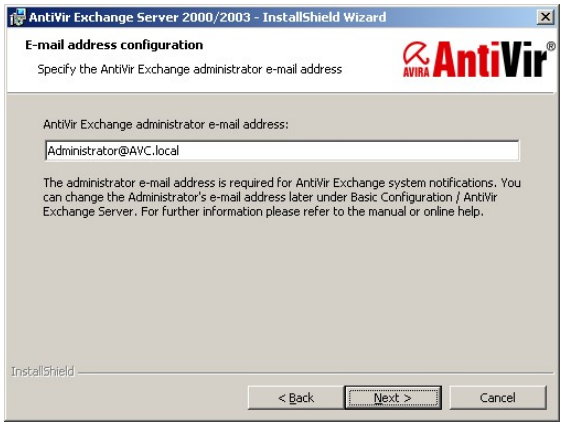


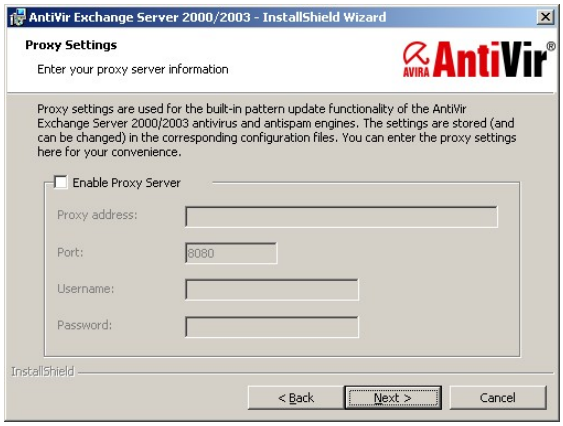
In this case, you can also configure the Client for Exchange cluster installations.

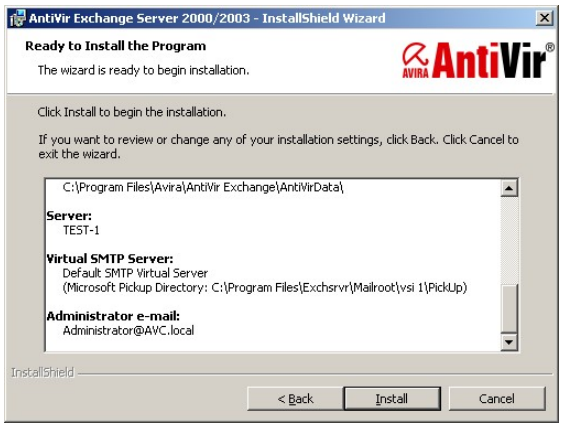
After confirming the mandatory license agreement, you can continue with the installation.



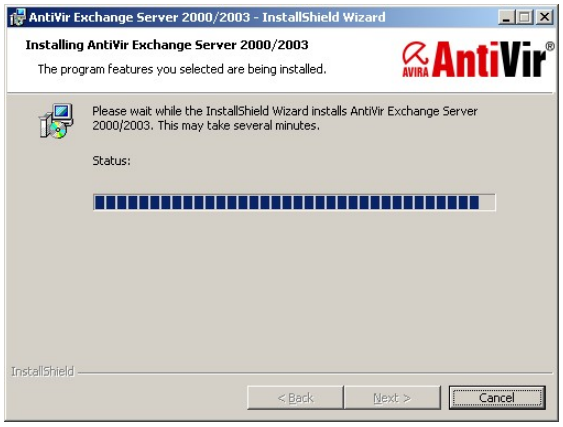
You can also use readymade configuration files if you have many Exchange servers at your site.

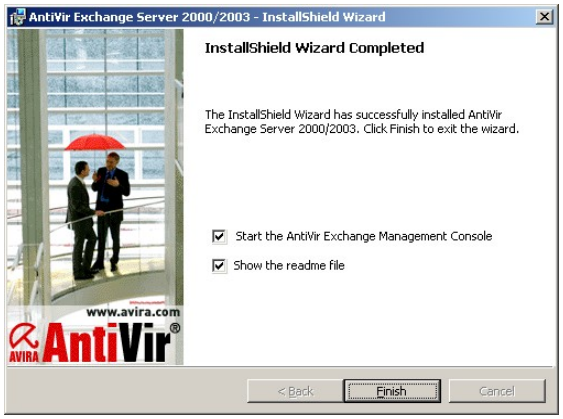




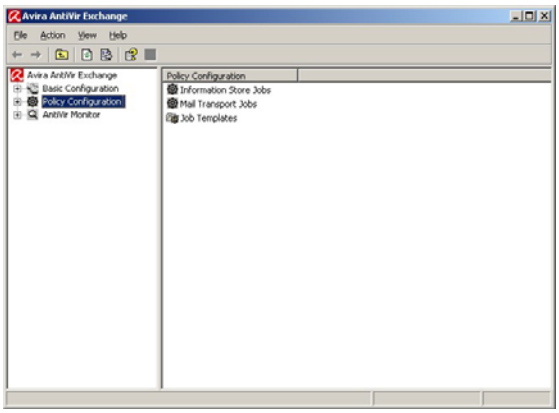


After selecting the Admin e-mail address and the proxy settings, a summary of the settings is displayed once again before the installation finally begins.





After the installation has completed successfully, you are asked if the Exchange Management console should be started.



This console, too, has been structured very coherently and navigating through it is a breeze.

Summary:

Manufacturer's website (www.avira.com):

The product also allows importing and synchronising the security environment with an AD he website is appealing and has been structured clearly. The site complies with the prevalent Internet standards.

The website itself gives you a clear overview of the current threats. It is possible to subscribe to various RSS news so that you are always kept up-to-date with the latest events.

In addition, the page has a security zone, where you can learn all about viruses and other malware.

The trial versions of the products are fully functional and run for 30 days.

The Installation Procedure:

The installation of the AVIRA suite is extremely simple and has been designed in a structured manner. The products have been named appropriately and after a quick look at the manual, you get to know immediately which file you need to begin with.

The installation wizard has been made simple to work with and there are not too many settings to be configured at this point of time.

The user can comfortably configure the parameters pertaining to the communication via the installation wizard.

The Server Management console requires a separate user. The product also allows importing and synchronising the security environment with an AD.

The update settings can be configured during this installation step itself. The default setting for the update is "daily". In our opinion, this should be set at least to "hourly" for corporate users.

AVIRA has the simplest and most user-friendly installation wizard of all products tested by us. As a result, you do not have many options to define the configuration settings.

After installing the products, you must start the Admin console manually, which is cumbersome. It would have been preferred if the console started automatically at the end of the installation procedure.

The first update must be carried out manually. It would have been desirable to integrate such a feature in the installation wizard itself.

The Administrator Console:

The administrator console conforming to MMC has been structured clearly and is easy to understand.

We were able to start the desired configuration even without referring to the manual, since the Admin console is structured in a very coherent manner. After creating the groups you can select the desired clients comfortably using a network browser and then initiate all actions via the pop-up menu. There is also an import wizard that allows to import from a CSV file or directly from an AD.

It would be practical to have a quick-start wizard, which guides the user with the initial steps.

The options for various settings are well suited to small and medium-sized networks.

Remote Installation

It is very easy to run the remote installation of the Clients. Here too there is no status indication. It is merely the display of a sandglass that indicates that the Client installation is in progress.
The remote installation itself is conceivably simple. You only need to configure the log-in account and select the desired package. No special preparatory steps are required. The Windows firewall on the Clients, unfortunately, must be configured manually in order to execute the remote installation.

There is no help function provided here!

License administration has been implemented in a comfortable manner and it is easy to configure.

Application Areas:

The AVIRA suite is best suited for Small and Medium Business, but fits also up to a max. of 20000 Clients. Especially for Small and Medium Business there is a special product Avira SmallBusiness Suite available that offers a configuration wizard that allows an easy setup, installation and configuration of the security environment. The settings options and, above all, the authorization settings of the Clients are inadequate for complex environments and enterprise-level networks and you can wind up with a marathon scrolling session with a large number of Clients.

The easily configurable suite demonstrates its strengths in an SMB environment.

AV Clients:

The message pop-ups are not an eye-sore. Unfortunately, you have to initiate the first update manually after installing the product successfully and starting it.

With the bare minimum of authorization settings, the user can do anything that he wishes to with the Client. In our opinion, this situation is a security lapse and should be changed at the earliest, since the user, in fact, has the authorization to disable the real-time protection.

In all other respects, the system has been structured clearly and you have an excellent overview of the system status readily available.

Conclusion:

The AVIRA product suite is very easy to install and leaves nothing to be desired.

The suite is appropriate for small to medium-sized networks. A search function allows filtering the environment for certain clients, groups, hostnames or IPs, however, for large networks a more detailed filtering method would be a desirable comfort feature.

The Clients do not need many resources and the remote installation procedure runs very quickly and in a simple manner.

There is no real-time status display for various actions. Hence, you do not know the precise and current status regarding the installation of products or updates. It would also be desirable to have a summary as the website of the console, which gives you information regarding the status of the Clients.

What also appealed to us is that a system check is executed after installing the console and, if the antivirus software is missing the wizard is started, which rectifies the problem.

Pros and Cons:

+ Client installation is fast
+ Admin console is structured clearly
+ Remote installation is easy
+ Good grouping functions are available
+ Installation effort is minimal
+ The website is good
+ Real-time status in the SMC

- No summary site in the console
- No administration of privileges at the Clients

Application Areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★★	★★★★	★★★

Brief Summary:

Installation Wizard	★★★★★
User Navigation	★★★
Administrator console	★★★★
Default Values	★★★★
MS Active Directory Support	★
Database Support	★★
Remote Installation	★★★
Website	★★★★★
Manual	★★★★

ESET

Test Software:

ESET Smart Security	→	Overall Endpoint Protection
ESET NOD32 Antivirus for Windows Server	→	File Server Protection
ESET NOD32 Antivirus for Exchange	→	Exchange Server Mail Protection
ESET Remote Administrator Console	→	Administration

Installation Procedure:

Downloading the Products:

The manufacturer's page has been structured neatly and coherently and it is possible to download the software without registration.

The time taken for downloads were as follows:

essbe_nt32_enu.msi
(35 MB) ⟹ 23 sec. (1.52MB/sec.)

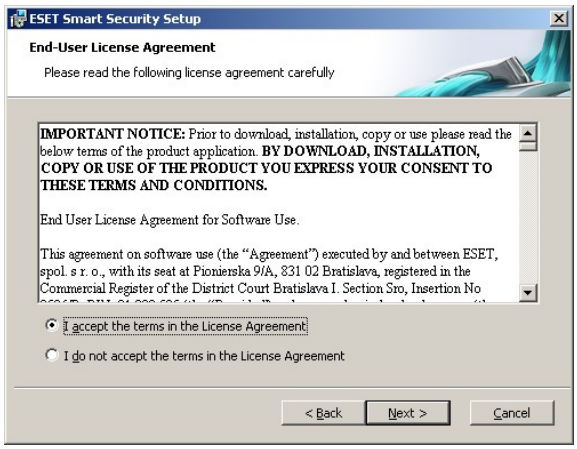
era_server_nt32_enu.msi
(22.2 MB) ⟹ 18 sec. (1.23MB/sec.)

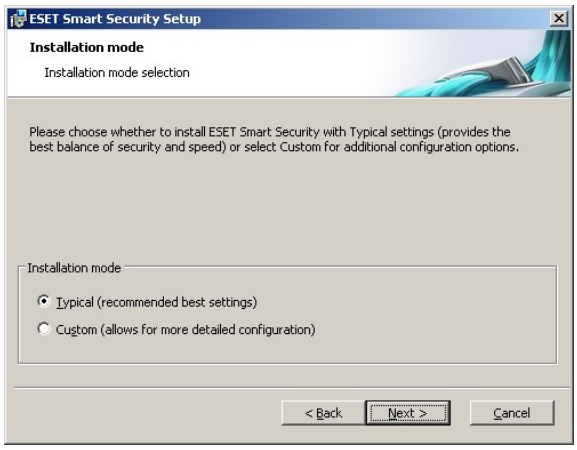
era_console_nt32_enu.msi
(14.3 MB) ⟹ 12 sec. (1.19MB/sec.)

Installing the Products:

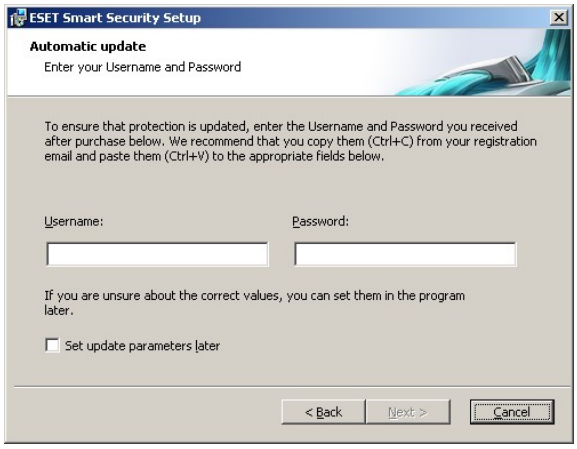
To begin with, you should take the manual and study it thoroughly. You can save yourself plenty of effort if you learn about the requirements of the Clients beforehand.

We begin with the installation of ESET Smart Security.

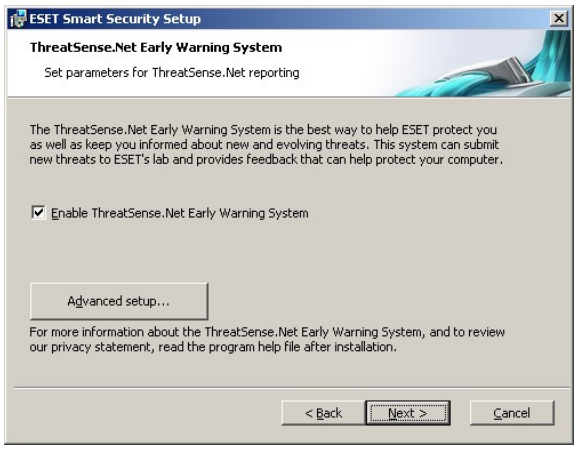




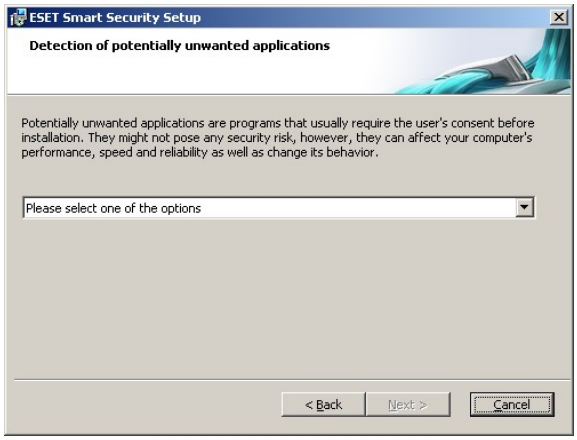
The default settings are a pleasant surprise for us at this stage.

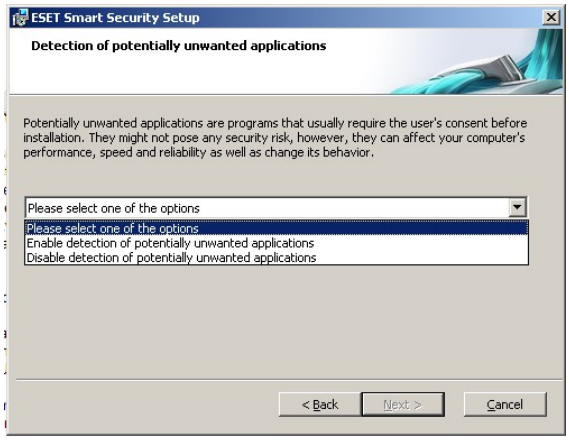


You can specify the registration information at the time of setup itself or you can enter these in the program subsequently.

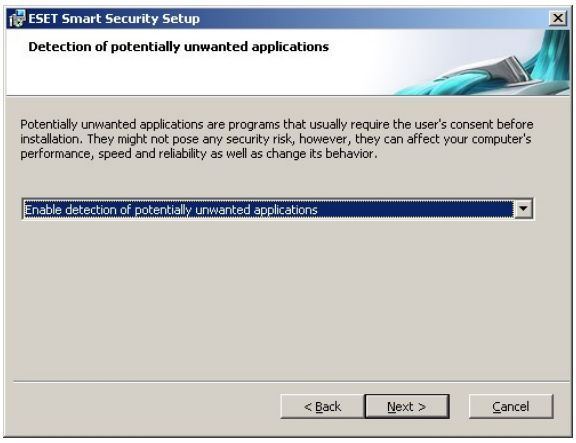


ThreatSense.Net integration is enabled by default. Every organization should make a decision regarding the data that is exchanged automatically, especially in high-end security environments.

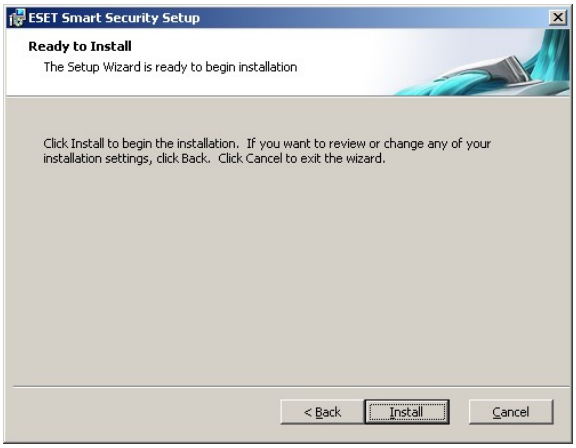


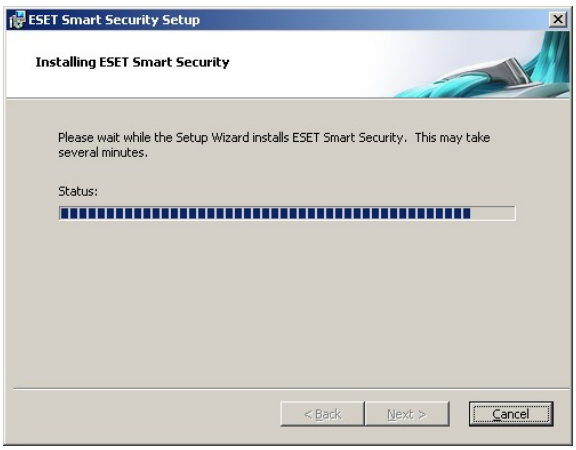


You can define certain rudimentary installation protection settings at this stage.

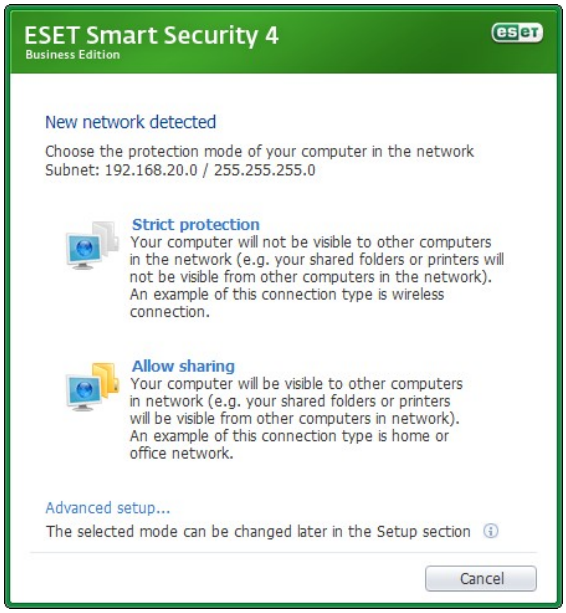


For the test carried out by us we enabled this protection.





The Smart Security suite welcomes you after the installation has been completed. There is no reboot required.

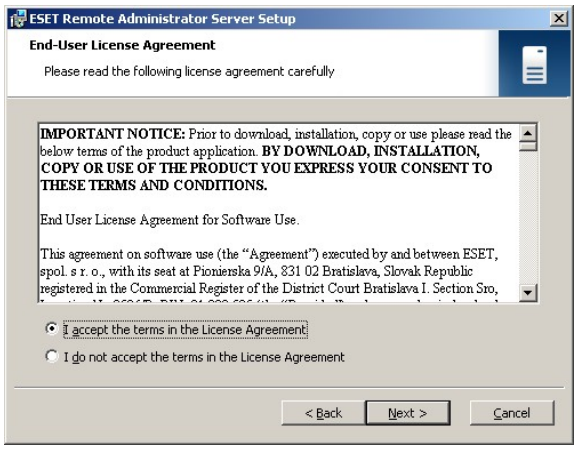


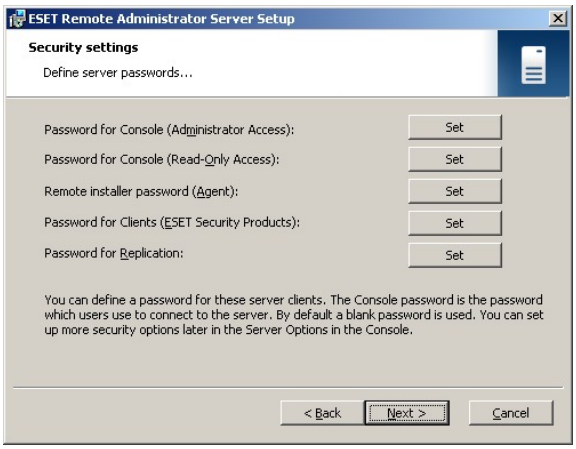
The Network Security screen is the next one displayed.

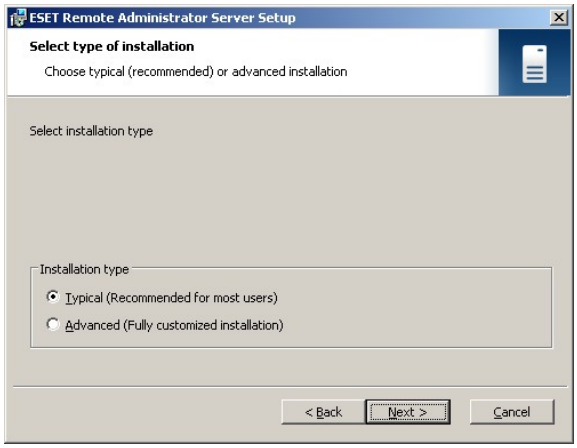
One potential issue we saw during testing is the firewall disables connections when prompting the administrator to set the protection level for the network. The administrator will need to set this manually. We think a better solution would be to configure this automatically during installation.

Messages appear on the taskbar and provide information regarding the status of the product.

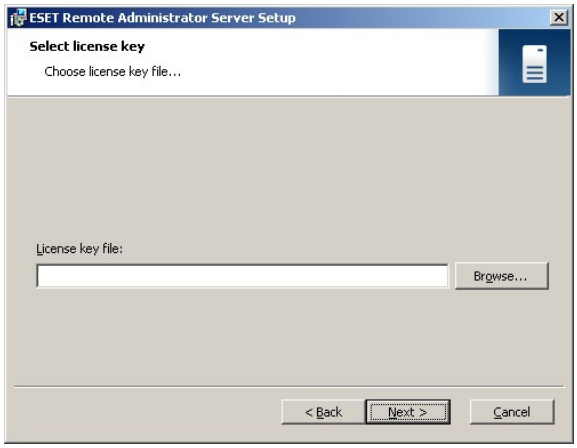
We shall continue with the installation of the administrator console.





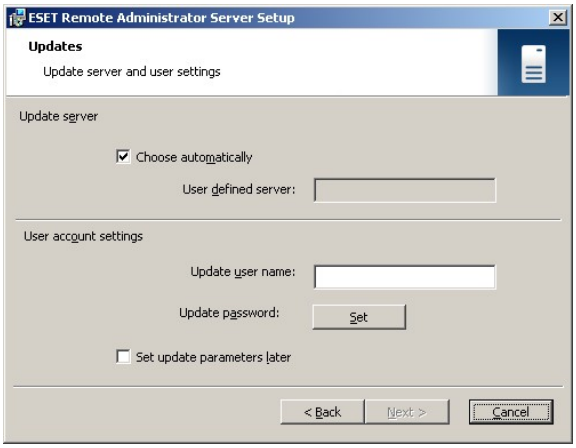


Here, too, we use the default settings for the purpose of our test.

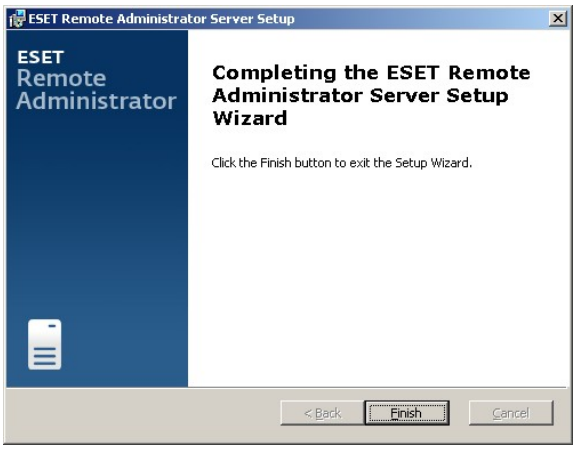


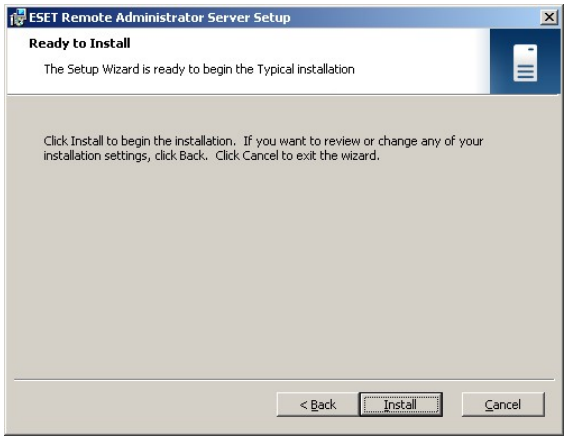
As in the case of Smart Security, you can specify the license file here.

This is where we came to the first obstacle. In fact, this is an elegant solution in which the Admin can specify different passwords for various modules, thereby assigning different roles to employees in complex security environments. However, the default settings are "Blank passwords" and when you continue with the installation subsequently, you need a password for certain modules. The password should be set at this stage of the installation in order to rule out the need for debugging at a later stage.

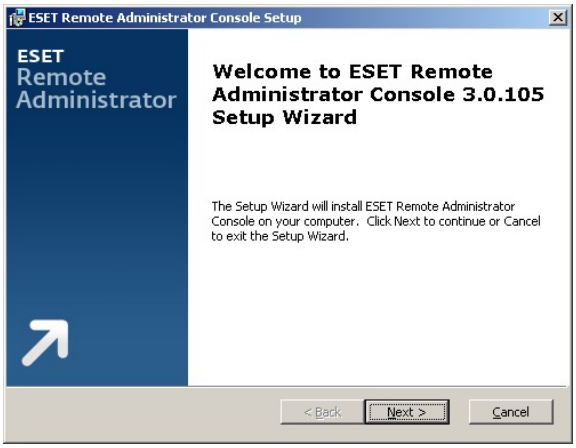


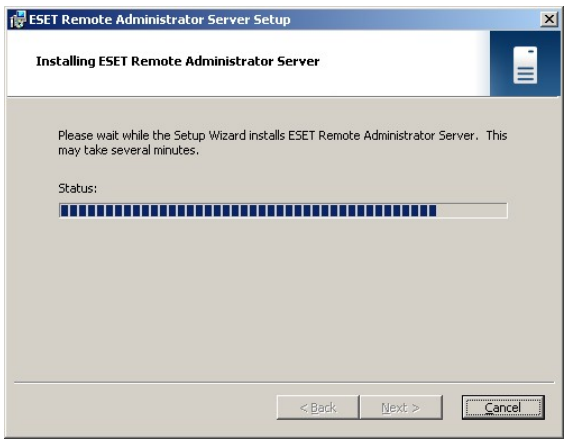
You can locate the update server in the next step and enter the required registration information.

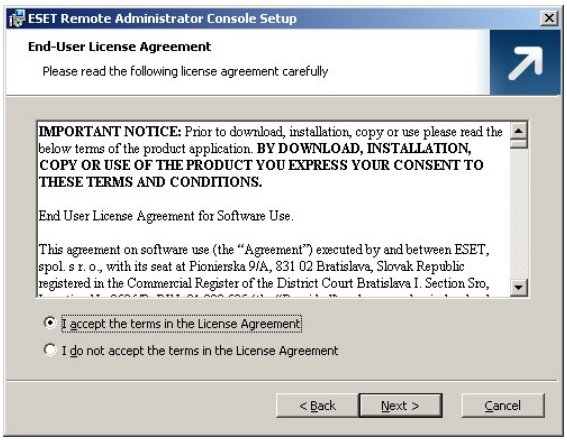


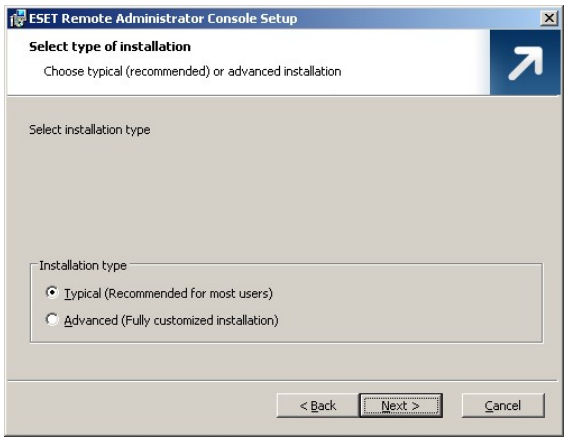


The installation of the remote administrator console is started immediately after completing the installation of the Remote Administrator Server:

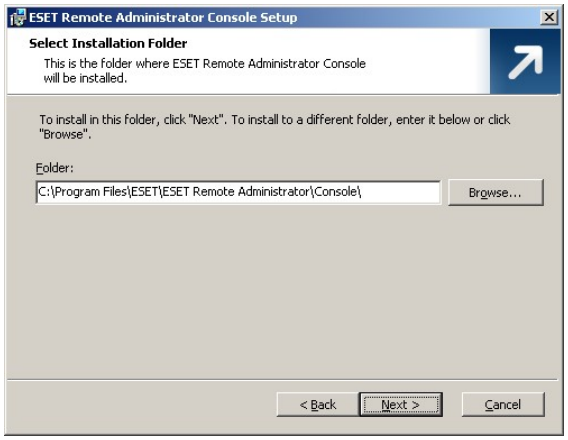


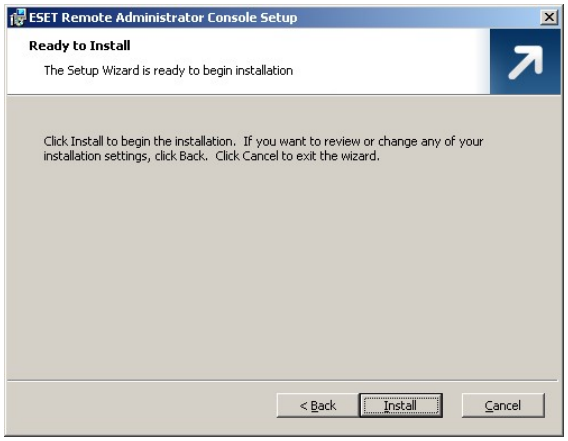




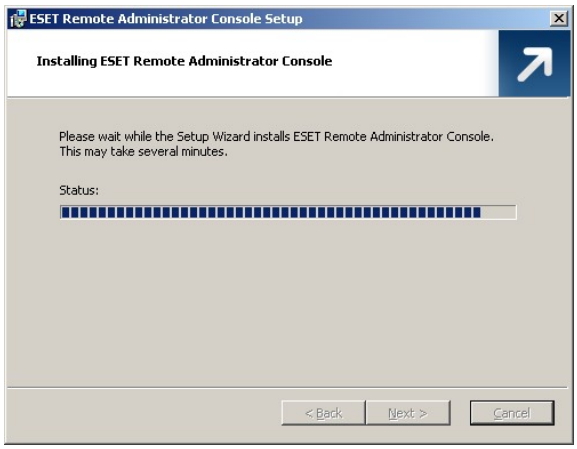


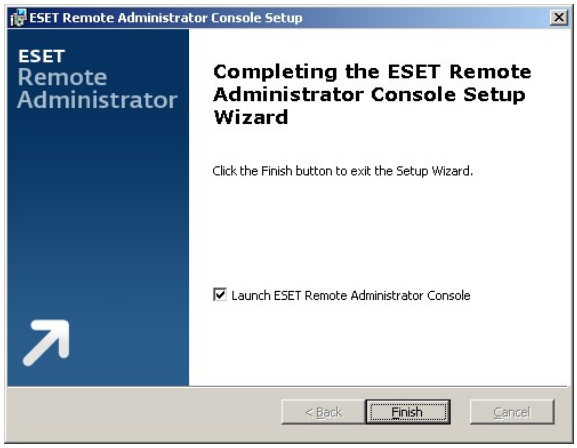
For the purpose of this test we used the default settings.



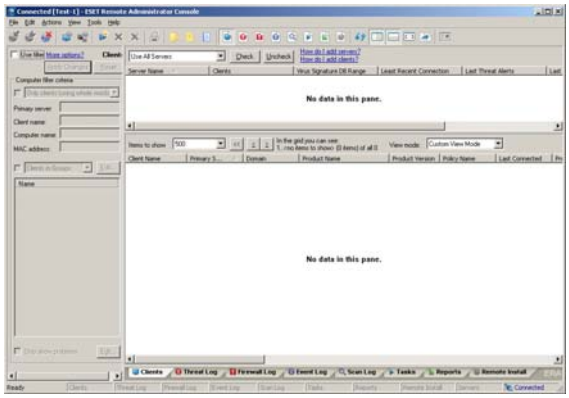


After confirming certain standard queries installation commences.

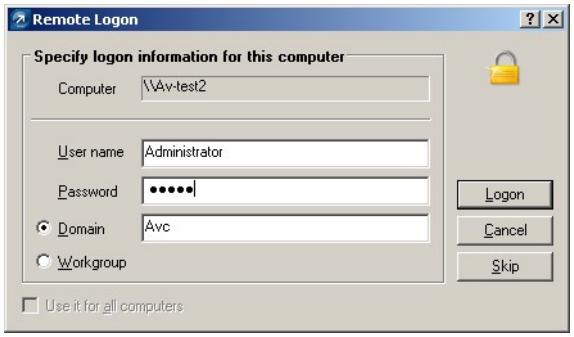




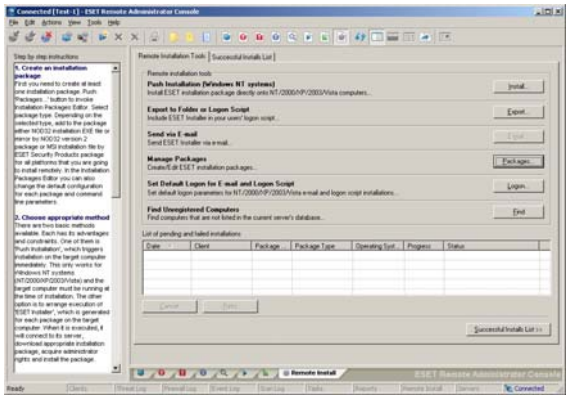
The remote administration console is started immediately after the installation is complete without a need to reboot.



What you would like to have here is an automatic Connect to the remote administrator servers. However, this has to be done manually.

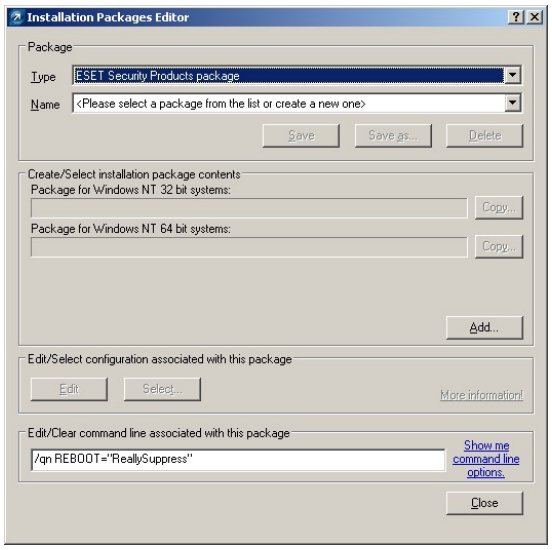


After establishing the link to the server, you proceed by clicking on the remote installation tab.

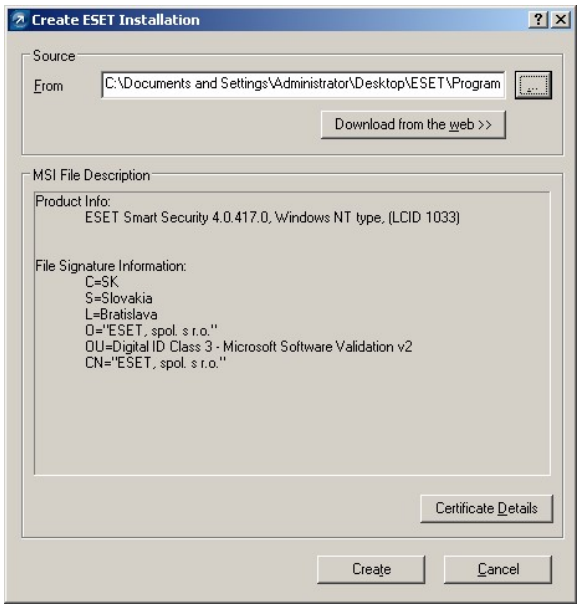


The variety of available options for remote installations is a good feature provided here.

We select the push method for our test. This option provides the push installation wizard. You can notice immediately that there are no limitations regarding the available configuration options.

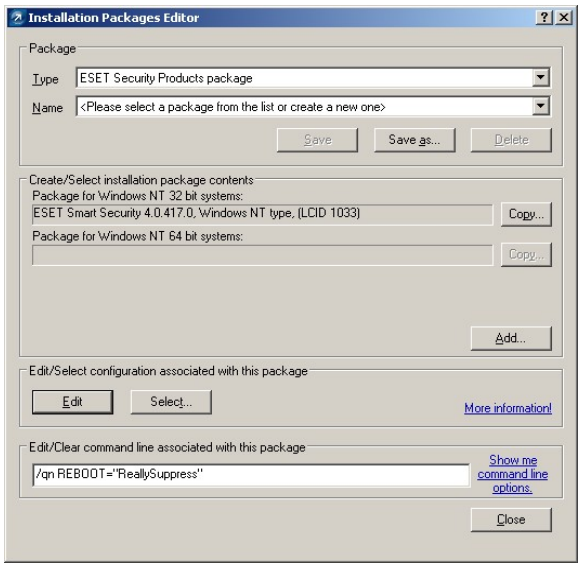


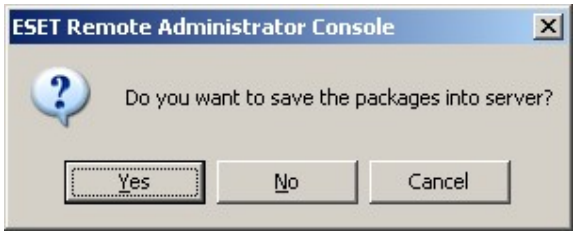
First, you have to set up an installation package. You have the option to fetch the package directly from the local PC or to download it via the Internet.



You can display all the necessary information about the MSI file selected using the MSI file description window.

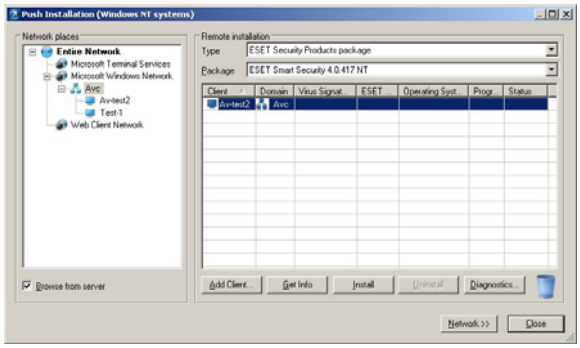
You can assign readymade configurations to various packages. The flexibility and configuration options are particularly remarkable and noteworthy here.

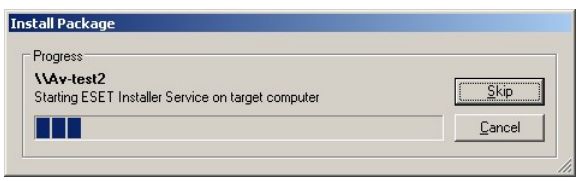


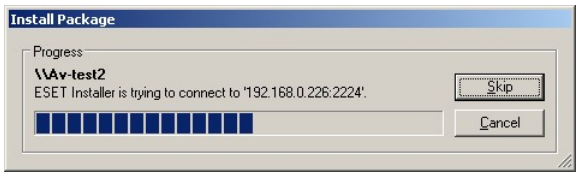


The packages are saved on the server after confirming the same.

You notice even with this list that ESET is ideally suited for very large networks.







There is a very elegant status display while the packages are being installed on the clients.

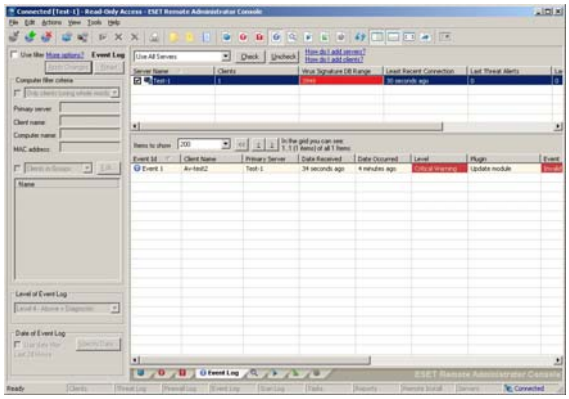
However, after the installation has been completed successfully, there is no option to select the update or to execute it.

The default settings for the clients select the ESET's Internet servers as the standard update server and not the management server defined in the network. You should change this setting since it is not desirable to fetch the signatures of each client separately from the Internet.

The greatest weakness of the ESET suite is undoubtedly the administration console, which has been designed in a very cumbersome and unwieldy manner. This console has the worst logging feature amongst all the products tested and there is no feature provided for real-time status updates. What is worse is that the status updates are sent from the Clients to the console 5 minutes after they are called up. You have, in fact, an update button provided, but this function is executed rather sluggishly.

In contrast, the filter options and display settings are exemplary – when it comes to networks containing many thousands of computers – this is where the options pro-

vided by ESET are definitely to be ranked at the topmost level.



Summary:

Manufacturer's website (www.eset.com):

The website has been designed elegantly. The site complies with prevalent Internet standards.

The website itself gives you a clear overview of the current threats.

Over and above this, the site offers removal tools free of charge for current threats.

The trial versions of the products are fully functional and run for 30 days.

Moreover, the website offers an on-line virus scanner and cleaner free of charge as well as a free process analysis tool (ESET SysInspector), which analyzes all running Windows processes and prepares a report of the same and removes them via Service Scripts.

The news relating to security on the website deals with general topics and is interesting to read.

The Installation Procedure:

The installation wizard has been structured clearly and various settings can be configured at the time of installation itself.

The installation wizard does not detect the OS automatically and uses the same policies for the server OS and the Client OS. This is a problem especially with network protection. As a result, you can quickly make the server inaccessible for the rest of the network. However, if the administrator wants to assure this does not happen and wants different installation packages to the servers and client OS, he can do so by changing the installation configurations.

The individual wizards for the management server and the remote administrator console respectively invoke the subsequent wizards, owing to which you do not need to look for the next module required for the installation.

The user passwords for various modules can be specified separately and independently. There is little Microsoft Active Directory support provided and, thus, though you can assign various tasks to different users, you cannot create any groups, which somewhat imposes limitations on the customization of responsibilities in complex and large environments.

The Administrator Console:

The real work begins after starting the remote administrator console. The options for remote installation are highly diverse and would practically meet any requirement. You need to define many settings before you can begin with the remote installation. It is a good thing, that ESET provides truly detailed documentation. It is absolutely essential to study the manual for this purpose.

The user navigation in the administrator console is not very intuitive at first and takes some time to get used to.

What must be highlighted is the excellent facility for filtering and grouping. The re-

mote administrator console is designed for administering very large networks having more than 100,000 users and beyond. ESET illustrates its real strength when dealing with networks of such large proportions.

Application Areas:

The ESET suite demonstrates its real strengths when even the smallest detail and most insignificant settings need to be configured and administered for many thousands of users.

The XML Configuration File structure lets the Admin customize every small detail even in the most complex environments and implement them across the entire structure.

When you are dealing with small to medium-sized networks, the configuration procedure might seems too cumbersome at first, but the installation package comes with a default recommended ESET configuration, which can be customized to make it work in every network.

It is helpful to plan the entire process of implementation to the finest detail, but majority of the configuration settings can be changed easily after the installation too.

AV Clients:

The Clients have been kept lean and offer all the required information and functions for the user.

Authorization settings can be adjusted to reduce the user privileges to a minimum.

The Client does not consume too much of the system resources.

Conclusion:

No other product offers as many customization features as ESET. Some preparation is required in order to execute remote installation on the Client computers. You cannot go very far by using merely the default settings, but they help speed up the deployment.

The implementation of ESET in a corporate network becomes a major project and requires detailed planning.

The menu navigation and somewhat crowded console looks complicated. You need to make sure to read the documentation before you start remote installation.

In our case it became necessary for the first and only time during the corporate tests to call up the hotline.

The policy editors are the most powerful amongst all the products that we tested. The unbelievable diversity and versatility of the settings throws light on the strengths of the suite. The ESET suite is best suited for very large networks and the most complex environments. You are definitely well-armed with ESET when it comes to providing an enterprise tool for security for the entire security department. Nonetheless, you must not underestimate the administration effort called for. The product could do well with simpler menu navigation.

Overall, you can say that ESET has enormous potential and makes an excellent proposal.

Pros and Cons:

+ Extremely diverse and versatile settings
+ Excellent options for remote installation
+ Client installation is very fast
+ Very good grouping functions
+ Excellent filtering options
+ Very suitable for the largest rollouts
+ Website offers many services free of charge

- Status updates in the console are cluttered and clumsy
- Console navigation is not comfortable and user-friendly
- Remote installation calls for extensive preparatory work
- Inadequate Microsoft Active Directory support

Application Areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★	★★★★	★★★★★

Brief Summary:

Installation Wizard	★★★★
User Navigation	★★★★
Administrator console	★★★★★
Default Values	★★★
MS Active Directory Support	★★★★
Database Support	★★★
Remote Installation	★★★★★
Website	★★★★★
Manual	★★★

G DATA

Test Software:

AVB10	→	Admin Console & File Server Protection
ClientSecurity10	→	Client Protection
MS10GER	→	Mail Server Protection

AV comparatives

Installation Procedure:

Downloading the Products:

Menu navigation provided by the manufacturer has been structured coherently and kept simple. You have no problems finding the desired product and you can download all the products with their full scope of functionality.

You can also receive updates via the Internet after registering successfully.

Using a 1.29 MB/sec. connection, the download times were as follows:

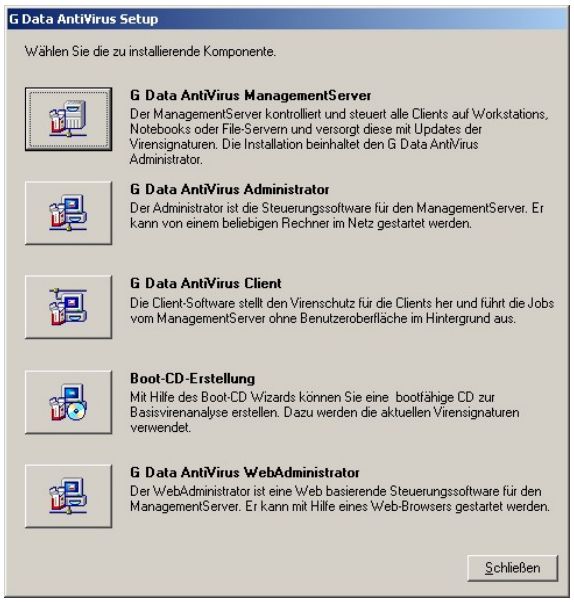
AVB10 (1.06 GB) ⇨ 19:20 min.

ClientSecurity10 (1.24 GB) ⇨ 20:20 min.

MS10GER (250 MB) ⇨ 03:12 min.

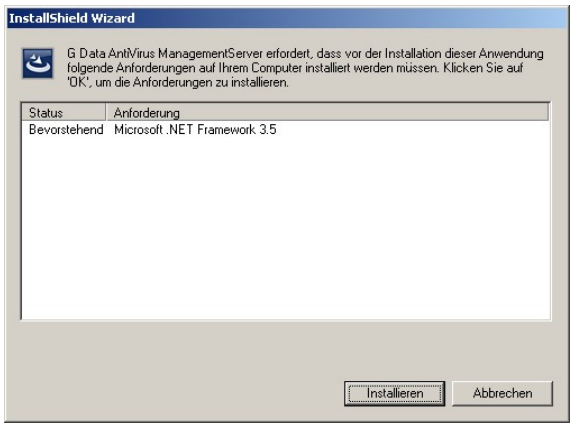
Installing the Products:

As the extremely large files seem to suggest, all products meant for the server need to be installed using an installation wizard.

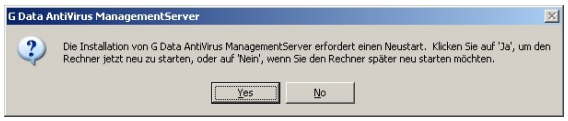


The menu navigation is exemplary and the individual modules have been provided with detailed and comprehensive clarifications.
As a result of the composition of the modules and clarifications given beside them, the sequence of steps required for the installation is also clearly evident.

We begin with the installation of the Management Server.

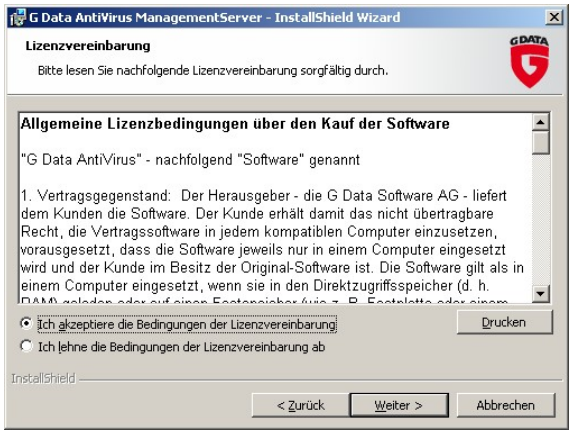


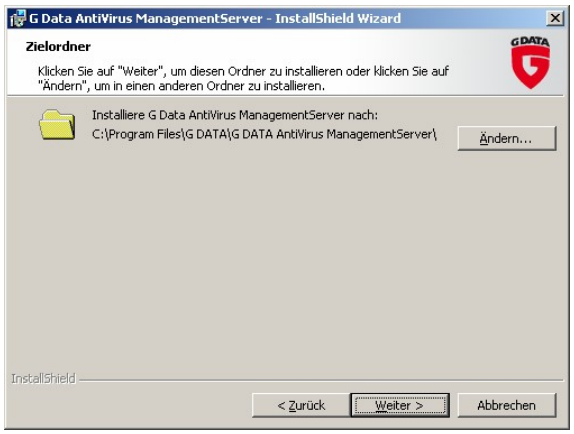
The Management Server requires the latest version of Microsoft .NET. This is supplied along with the installation package and, hence, you do not need to download it manually.



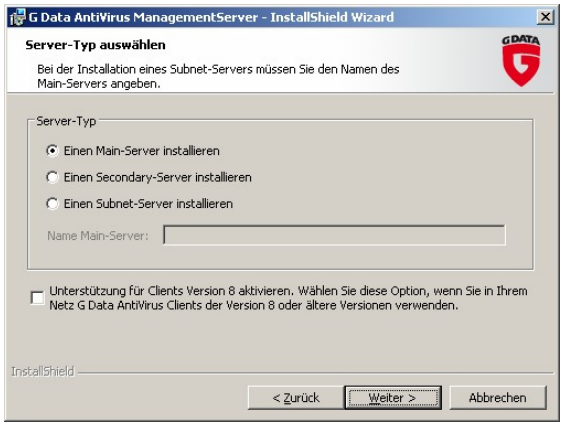
Administrators are not very pleased to see this message since the IT is active at this point of time. But the reboot is only necessary if the .net Framework was not already installed on the computer.

You expect the installation wizard to return after MS .net 3.5 has been installed successfully and the server has been restarted.





We let the default values be used for the standard query regarding the license agreement and the installation folder.

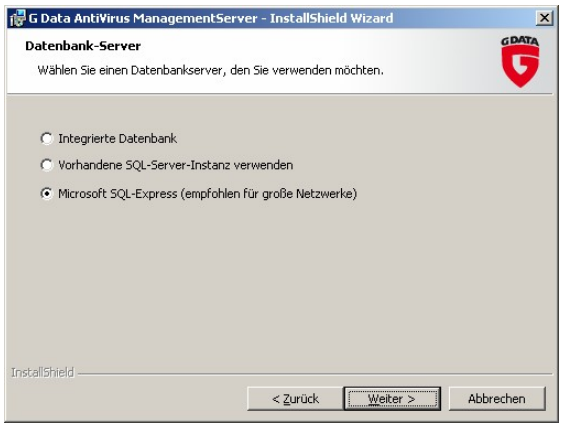


You should select the type of server in the next step. You can immediately notice here that it is no problem whatsoever for the GDATA suite to be deployed in large networks having branch offices and decentralized Servers. We select "Main Server" since it is the first installation in our network.

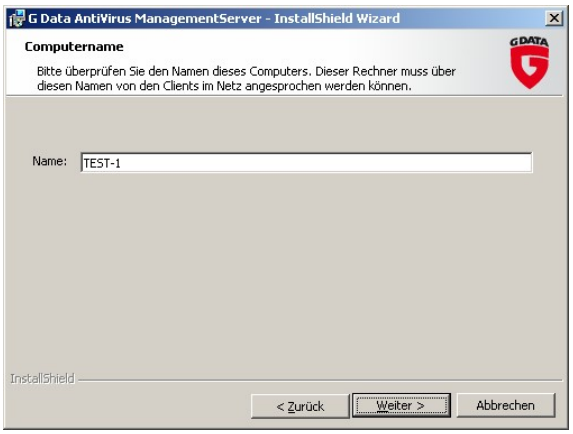
We select the desired database server for the suite in the next step. The message that SQL Express is recommended for large networks is somewhat misleading. This statement is applicable if there is no instance of an SQL Server in the existing network, or the existing SQL Server has enough to do with the existing databases.

However, it needs to be mentioned here that the Express variant of the MS AQL Server is naturally not comparable to the large variant in terms of performance.

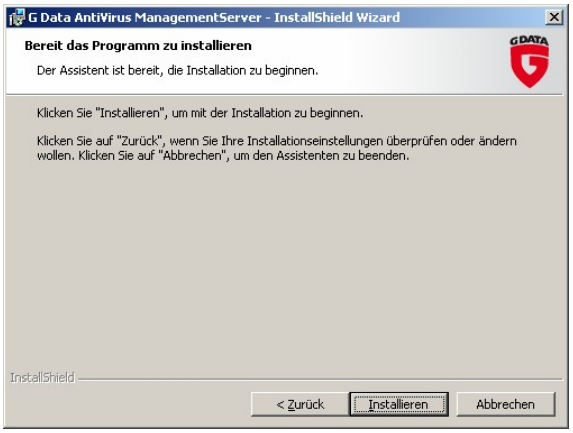
This system does not provide any support for open-source databases such as MySQL.

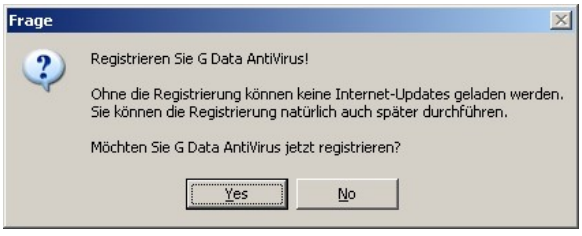


For this purpose, the powerful Installation wizard of the GDATA suite contains the MS SQL Server Express installation packages.



In the next step, you need to convey to the installation the network name with which the Management Server can be accessed.
You can kickoff the installation procedure after all the information has been collected.

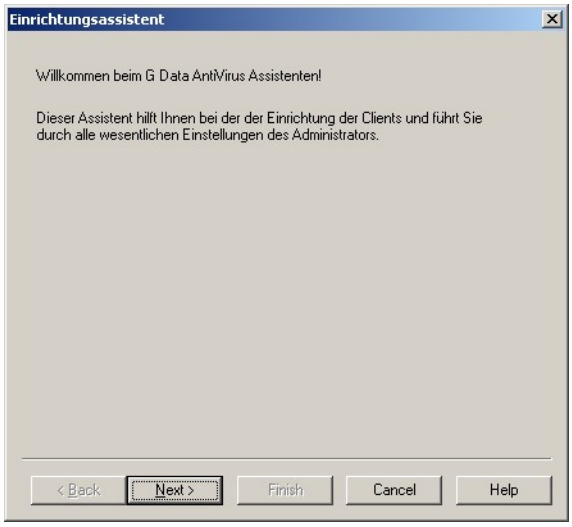


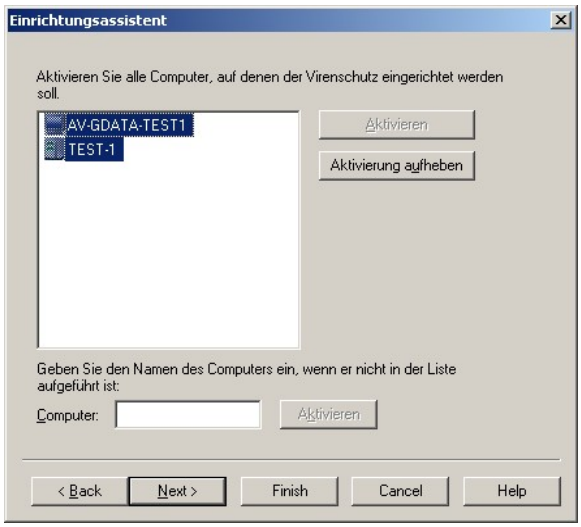


After the installation has been completed successfully, the message regarding regis-

tration is displayed once again to make the system ready to accept updates.

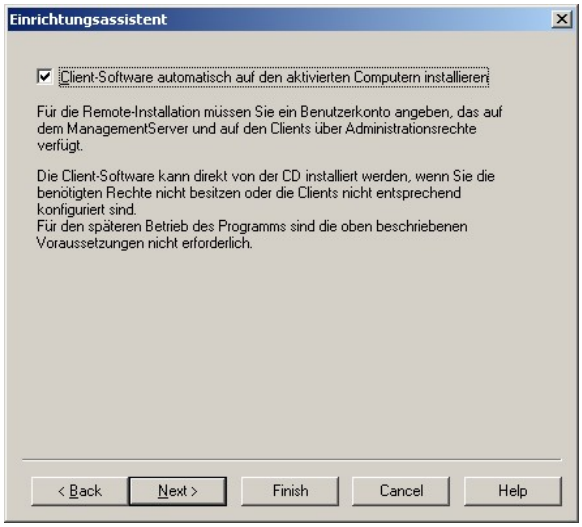
Immediately after installation has been completed, the "Setup Wizard" appears:

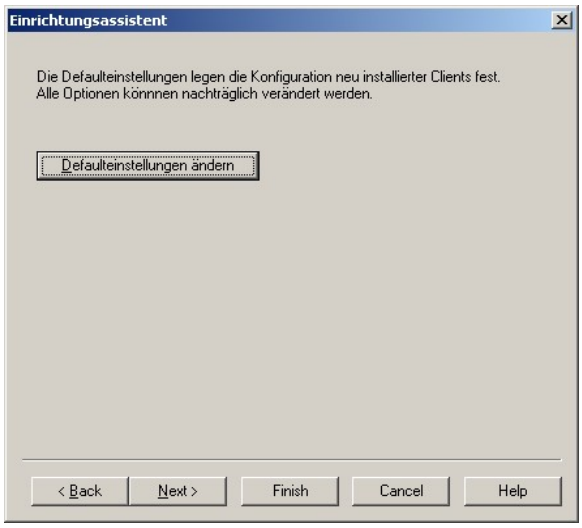




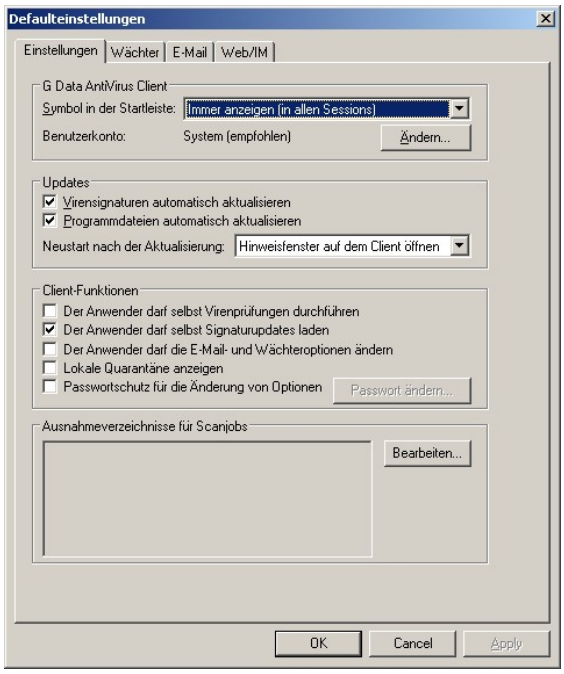
The wizard displays those computers, which do not yet have any GDATA products installed, without the need for anything much by way of configuration and based on the network environment and the AD.

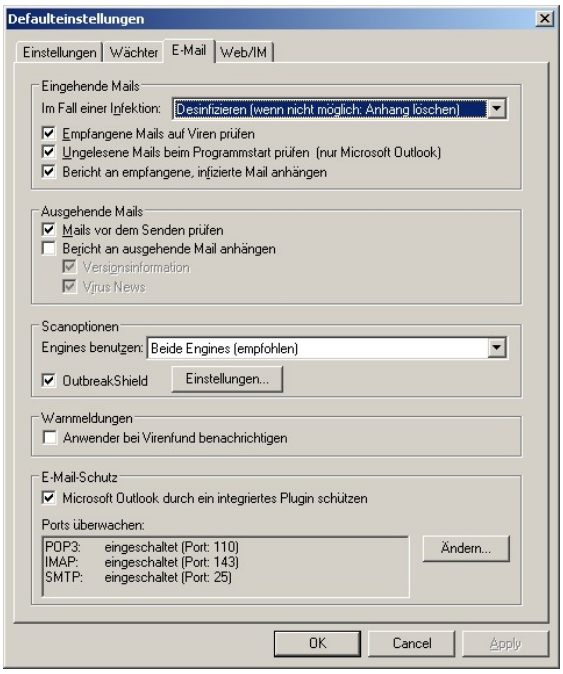
The description of various menus is exemplary and you can dispense with the manual completely as an aid for the installation procedure.

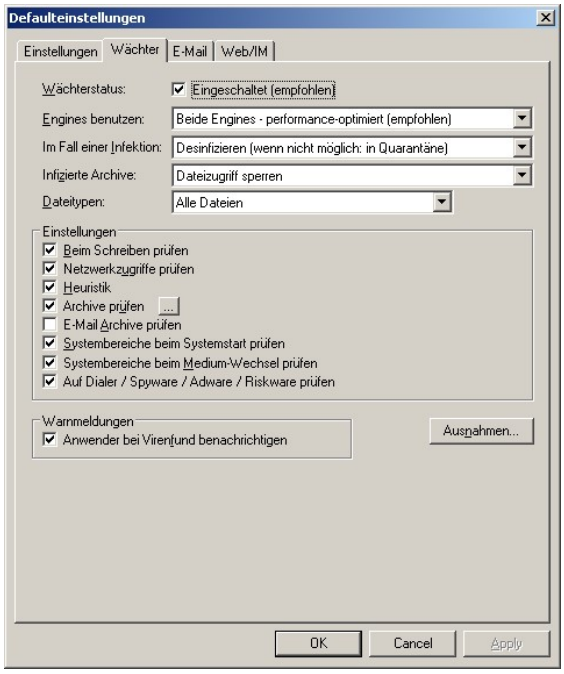


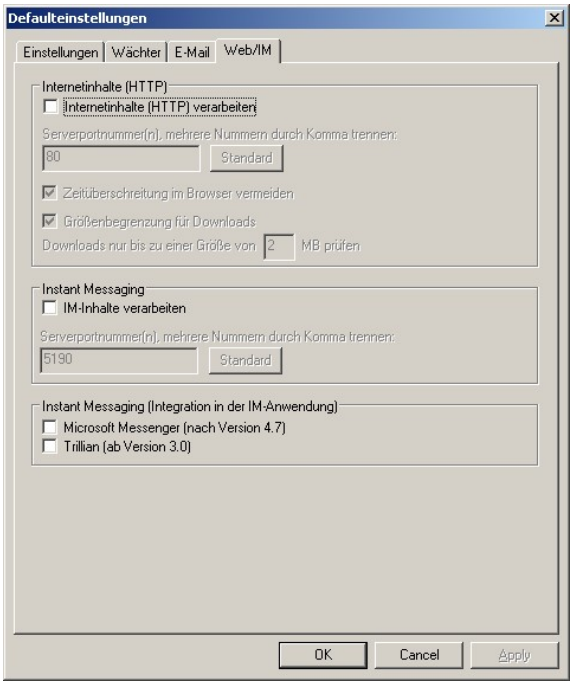


You can configure the default settings with the help of the wizard.

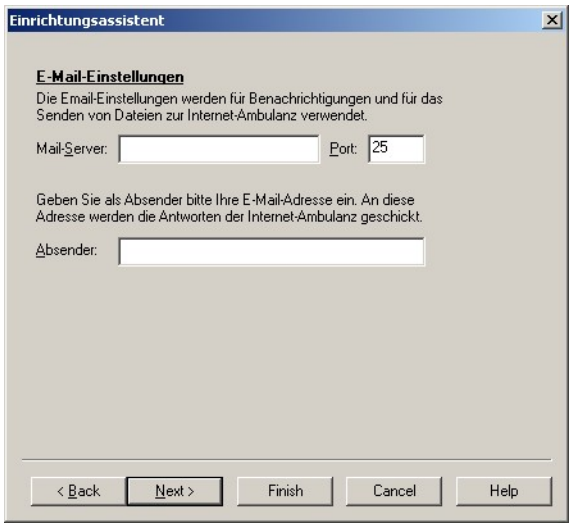




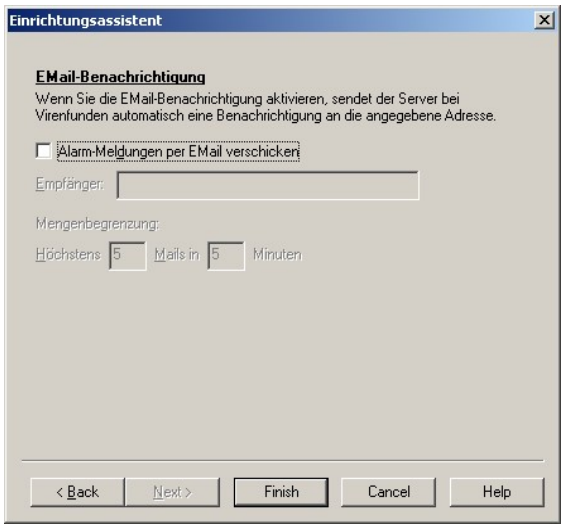




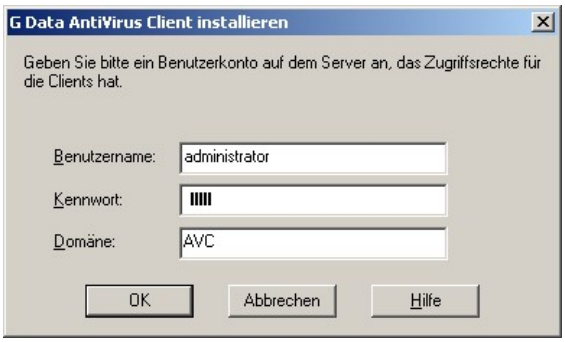
The wizard does not leave anything to be desired, and despite this, it is structured in a simple manner, and yet incorporates all features that are required.



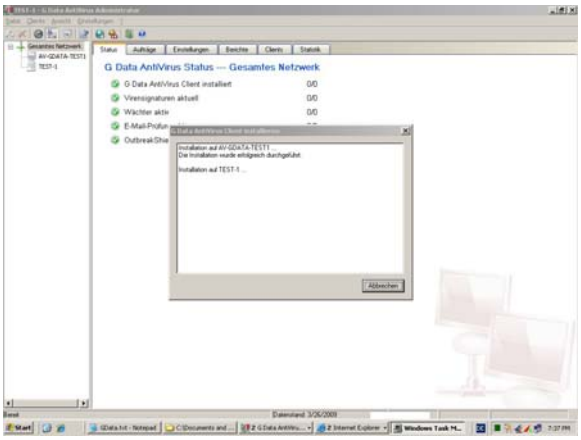
In the next step, you can specify the e-mail address to which messages should be sent. This address is used for comparison with the GDATA Internet Ambulance.



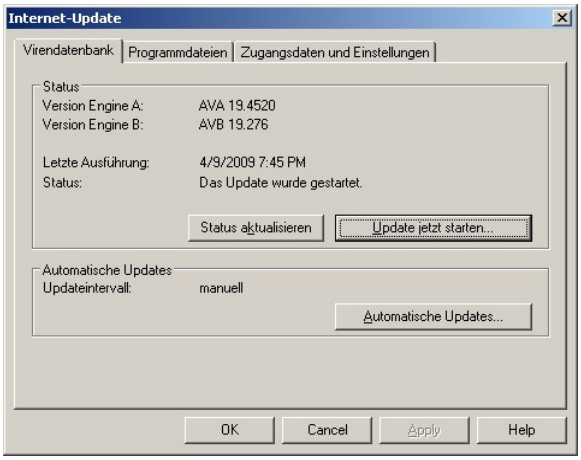
You can also specify a separate address for the alarm messages. You can see here that the GDATA suite feels very comfortable even in complex security environments and gives the administrator the option to configure his department optimally for the security issues and concerns.



Here, you should define the account with which the Clients would be installed and configured. The system provides MS AD support.



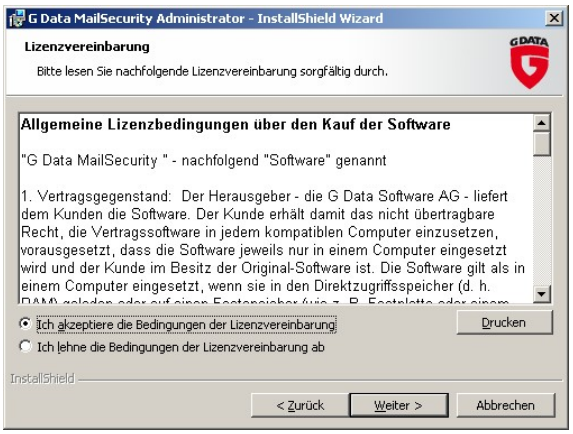
After the Setup wizard has completed its task, you can start with the installation of the software on the Clients and Servers selected earlier.

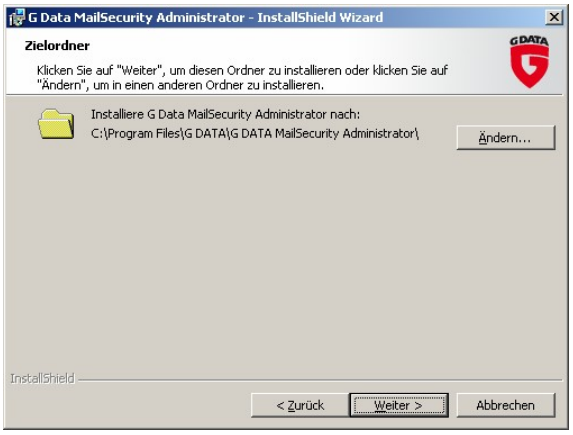


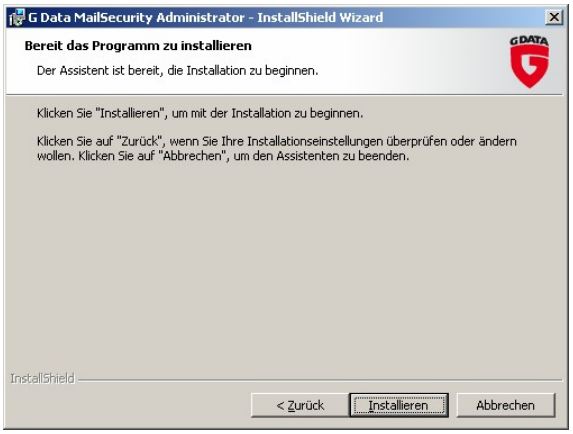
The settings of the update method too have been designed coherently and kept simple.

Navigation within the Management Console leaves nothing to be desired and is self-explanatory. It has been kept lean and simple and yet includes everything that you require.

In the next step, you install the Mail Server protection.





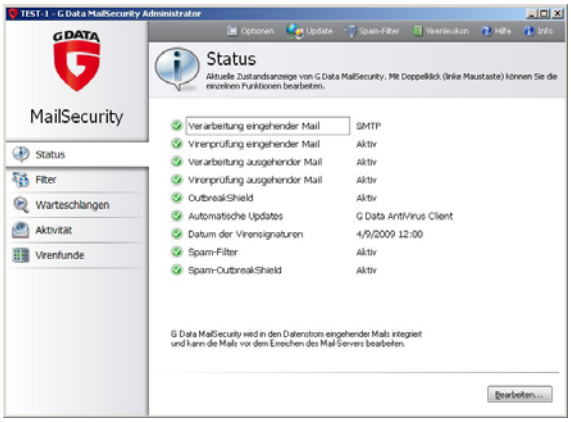


After completing the standard installation with the usual queries regarding the license agreement and the destination folder, a login window appears at the Mail Admin console.

You also need an SQL entity here for the statistical evaluation of the mail traffic. You can, of course, use the SQL Express server that has been installed previously.

GMail also detects immediately that a GDATA Antivirus Client has already been installed on the Server and then also uses these signatures.

After logging in to the Administrator console of the GMail Security Scanner, you are presented immediately with an overview of the processes running currently and other system information:



Here too, the graphical user interface leaves nothing to be desired as far as user-friendliness is concerned, and, at the same time, all required settings can be configured.

Finally, you would get a message regarding the successful registration on the GDATA update server:

Summary

Manufacturer's website (www.gdata.de):

The website has been designed elegantly and you can find your way around it easily. The site complies with the prevalent Internet standards. The navigation has been structured coherently and kept simple.

There is an on-line shop, but this merely refers you to the nearest reseller.

This system has its own security zone (threads), in which you can get an overview of the threats from the Internet and a tip on the product that provides protection against the same. The zone provides detailed information regarding the threats and a glossary simplifies the task of users who are not well versed in the subject.

The Installation Procedure:

After downloading the unbelievably large size of installation files, 2.58 GB the Admin expects the very elegant and sophisticated installation wizard.

The products have been assigned relevant and appropriate names with which you need to start.

In the first step, you are required to update the server to Microsoft .NET version 3.5. This update is included in the installation package of the suite. Unfortunately, this update requires that you restart the server.

After the restart, the installation wizard starts before establishing the network connections. This is where you understand why the installation file for the suite is so huge.

The installation wizard has been designed perfectly and leaves nothing to be desired. The system can detect immediately whether you would like to install a Slave Server or a Main Server. This is where you realize that the suite is also suitable for large networks having branch offices.

Good database support is also available. You can choose between an integrated database engine, a new SQL Server entity or the MS SQL desktop engine. This setting is also the default setting. The tip that the SQL desktop engine is recommended for large networks is in our opinion superfluous, since a dedicated SQL server performs definitively many times better than the desktop engine, with the only exception being that the network traffic is naturally reduced.

After the installation is completed, the wizard guides the Admin through the registration process, without which no updates would be possible.

First, the Setup wizard welcomes the user, with this welcome window blending very elegantly into that of the installation wizard. Even here, we do not find any setting options that are not included.

The entire installation wizard, right up to the completion stage, is designed very coherently and with a simple structure, and you can configure the most important settings in a matter of minutes.

In our opinion, the installation wizard and the wizard of the GDATA suite are the best available in all the products tested by us.

Support for Microsoft Active Directory is provided and the default settings used for all modules practically do not need to be changed at all.

The Administrator Console:

The console has been designed extremely well. You can find your way very quickly as a result of the arrangement similar to that of the MMC and the tabs on the right side guide the user quickly to the desired functions.
The console has been designed in a very appealing and elegant manner, which makes working with it a very comfortable experience.

The status page of the console could have been designed to be more detailed and contain more information.

However, as in the case of KASPERSKY and SYMANTEC, there is no cause for complaints in connection with the functionality and the organization of the Clients. We also found the console to be very appealing and attractive.

Application Areas:

The entire GDATA suite can be used without any qualms in all sizes of networks. You can also operate all branch offices well by conserving network resources owing to the master-slave configuration.

You are also equipped for large networks by means of the database support.

AV Clients:

The message pop-ups are not an eye-sore. After installing the product successfully and starting it, the system executes all the steps necessary automatically.

The user can configure only the most important settings with the least of user privileges.
The Client has also been designed elegantly and appealingly and you can find your way around it almost immediately.

Conclusion:

The GDATA products are extremely mature and well developed. This is true, starting right from the installation wizard, which practically never lets the Admin scratch his head, right up to the comprehensive configuration options, which cover all requirements even in more complex environments.

The only issue about which you can complain is that of missing real-time logging functions, which enable an Admin to know exactly about the update and configuration process of his Clients.

It would have been nice even to have an overview page depicting the status and condition of the Clients.

Apart from these considerations, we can recommend the GDATA suite strongly to any Admin. The product is also reasonably priced.

Pros and Cons:

+ Very good installation wizard having excellent user navigation
+ MS Active Directory Support
+ Client installation is fast
+ Admin console is designed clearly and coherently
+ Remote installation is very easy
+ Manual is not necessary
+ Also suitable for larger rollouts
+ Good database support
+ Good quality of the manufacturer's web-site

- No summary page in the MMC
- No proper real-time logging feature

Application Areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★★	★★★★★	★★★★

Installation Wizard	★★★★★
User Navigation	★★★★
Administrator console	★★★★★
Default Values	★★★
MS Active Directory Support	★★★★
Database Support	★★★★
Remote Installation	★★★★
Website	★★★★
Manual	★★★★

Kaspersky

Test Software:

Kaspersky Antivirus for Windows Workstation	→	Client Protection
Kaspersky Antivirus for Windows Server	→	File Server Protection
Kaspersky Antivirus for Microsoft Exchange Server	→	Exchange Server Mail Protection
Kaspersky Administration Kit	→	Administration

Installation Procedure:

Downloading the Products:

The manufacturer's site has been designed very elegantly and you have an overview of all current threats, which are presently circulating on the Internet along with the relevant and appropriate tools to combat them.

The download times were as follows:

kav.6.0.3.837_winwksen.exe
(59.3 MB) ⇒ 01:36min. (633 KB/sec.)

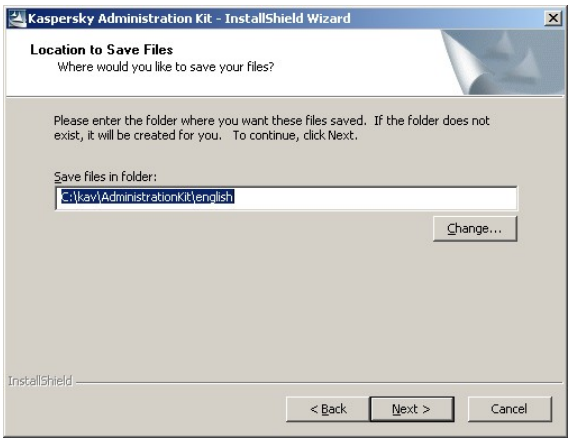
kav.6.0.3.837_winserven.exe
(55.1 MB) ⇒ 01:31min. (620 KB/sec.)

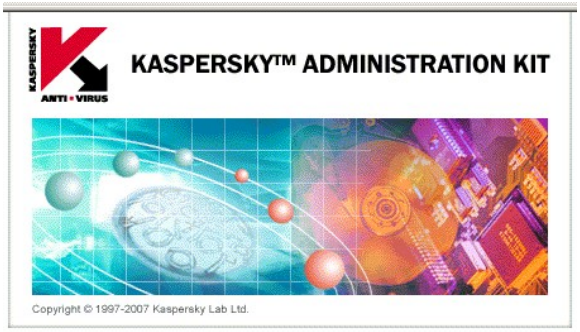
ks5.5.1388.0_exchangeen.exe
(41.7 MB) ⇒ 56 sec. (764 KB/sec.)

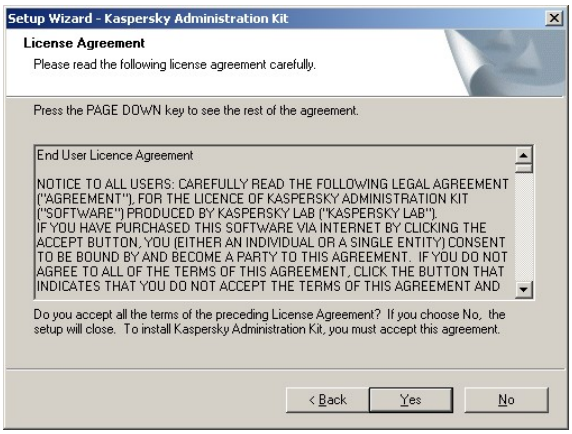
kasp6.0.1710_adminkiten.exe
(40.7 MB) ⇒ 54 sec. (772 KB/sec.)

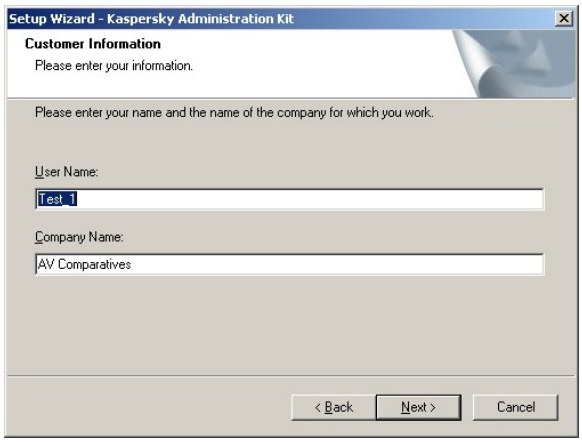
Installing the Products:

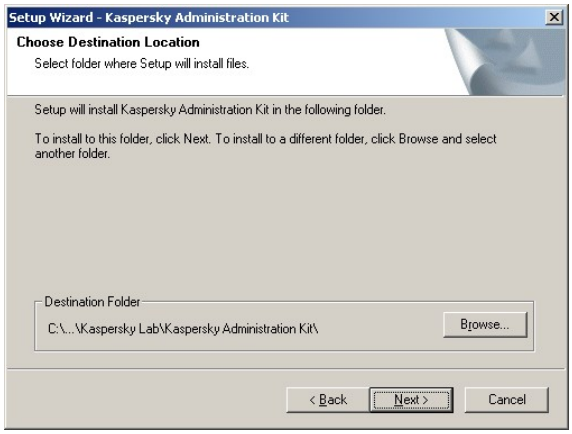
We begin with the installation of the Administration Kit.

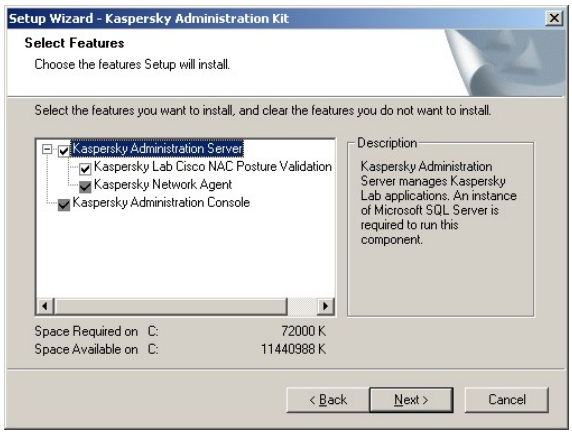






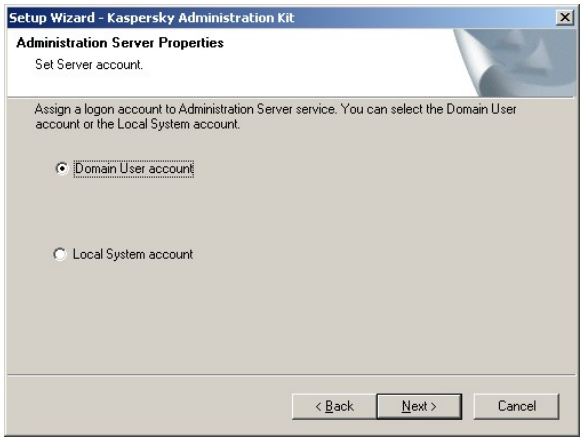






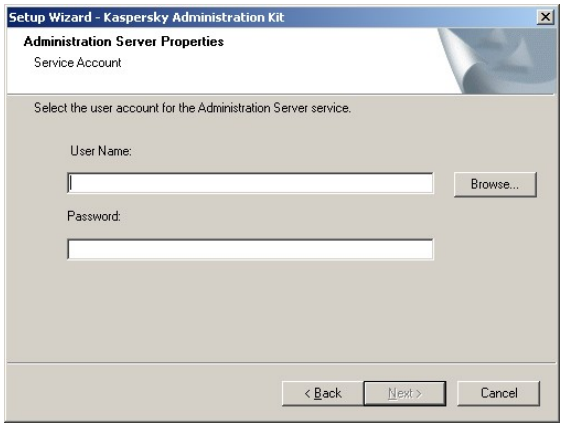
A message regarding the missing database is displayed after the standard queries initially.

However, as you can see, you can install the MSDE immediately using the Administrator Kit.

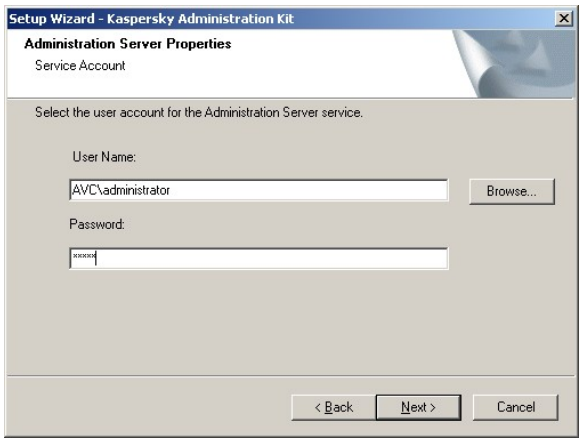


This is where you specify the user details for logging in to the administrator services.

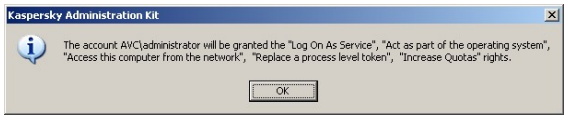
You can only select the system account or the domain account logged in at present. It would have been desirable to have better AD support here in order to be able to select Admin groups as and when required.



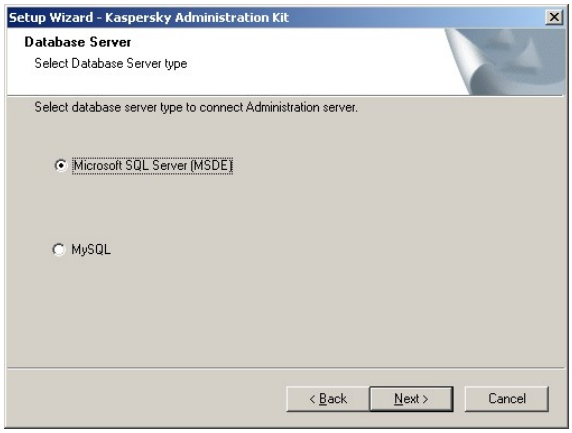
What is good here is that you can link the services account separately to a user.



For the purpose of our tests, we have used the administrator account of the domains for the sake of simplicity.

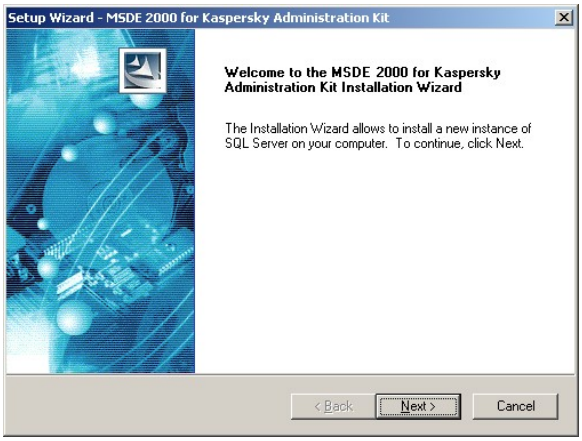


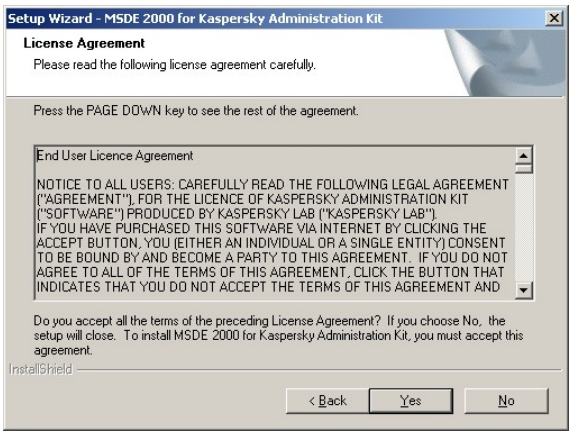
Information that is displayed about the actions is detailed and comprehensive. You have an immediate overview of the additional privileges that have been assigned to this service account.

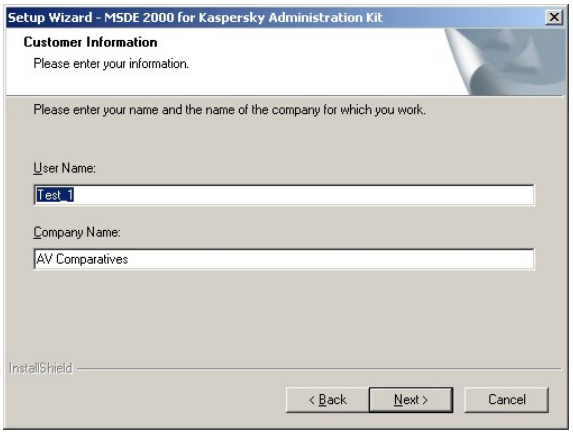


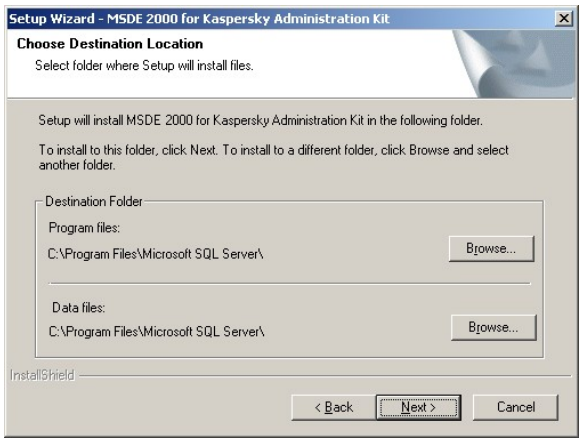
The fact that the system supports the open source database, MySQL, is also a nice feature.

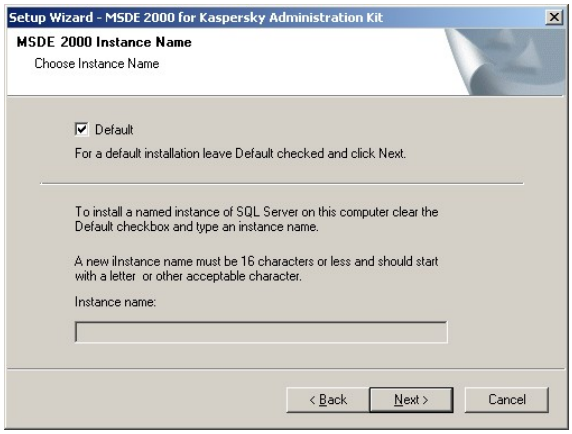
For our test, we have selected the MSDE recommended by default.

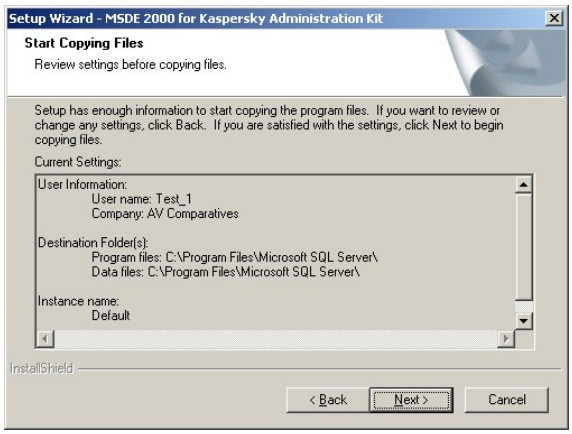






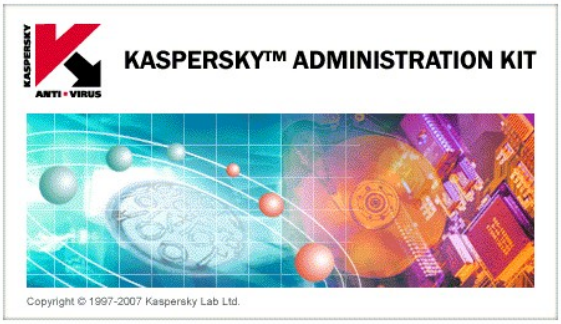


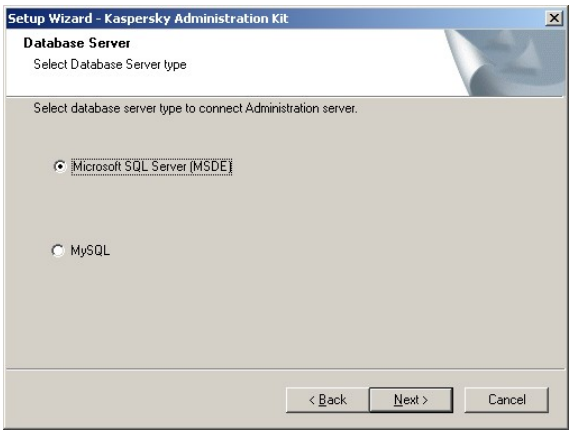




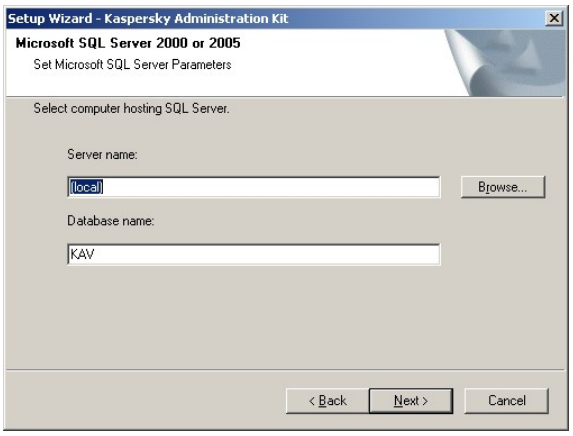
When installing the MSDE, you have the option to configure the important settings for the Admin, such as, for example, saving the database file to another destination.

After installing the MDSE or optionally, MySQL, the actual installation wizard of the Kaspersky Administration Kit starts up.

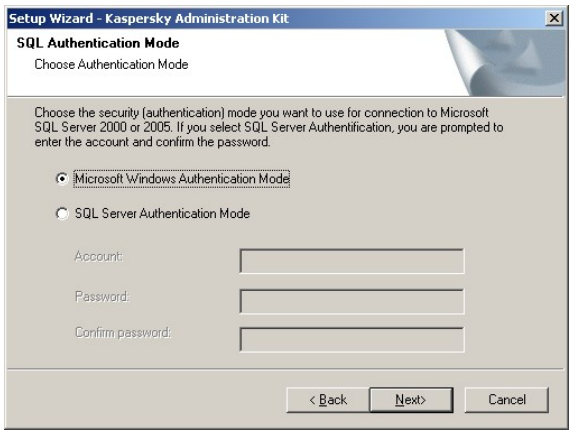




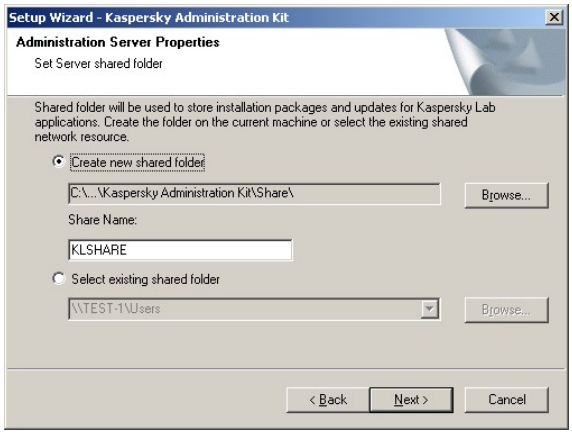
You can specify the type of database here once again.



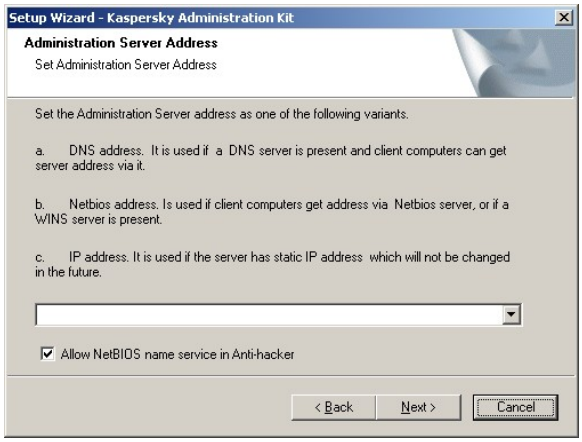
We retained the default settings at this juncture.



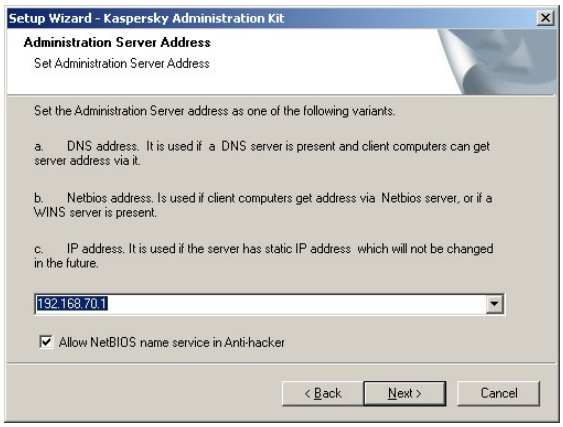
The system confirms the authentication – and the procedure moves to the next step.

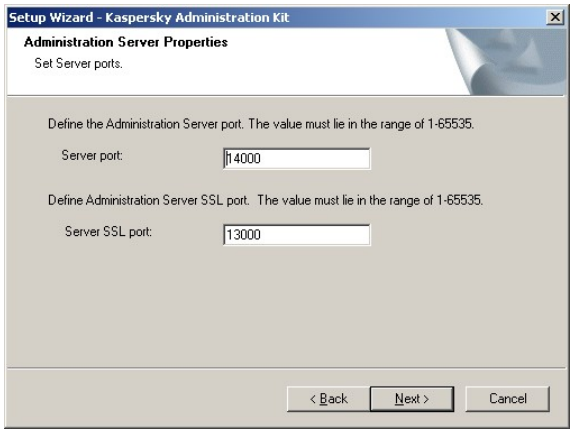


This is how it should be: The wizard helps you with the setup of the network share for the installation files of the products, which can be distributed using the Administration Kit.

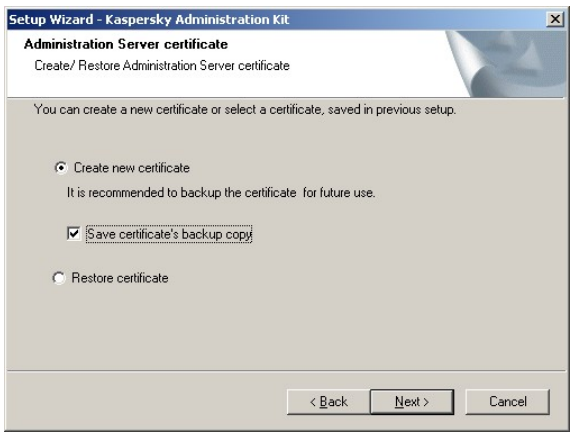


There are good options available for selection. The IP address function is very comfortable, since it is often necessary to assign two different IP addresses to servers, and you can select the desired one here.

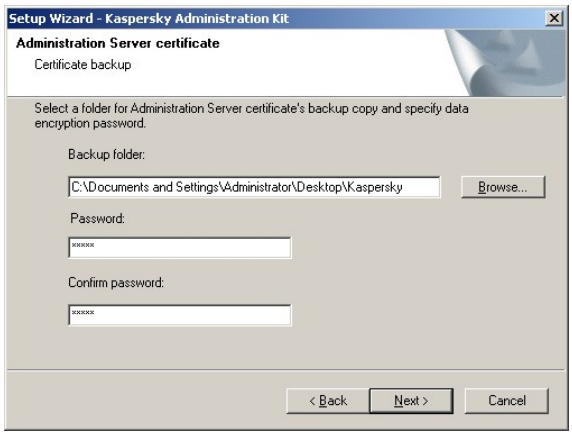


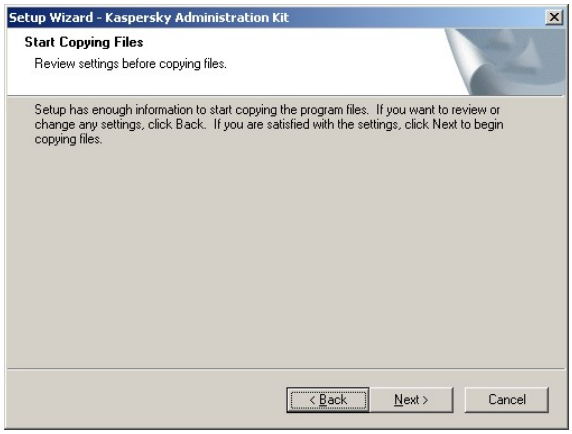


You can even assign the communication ports at the time of the installation based on the specifications of the Admin.



Finally, you also get to see X509-certificate support with such an AV suite.



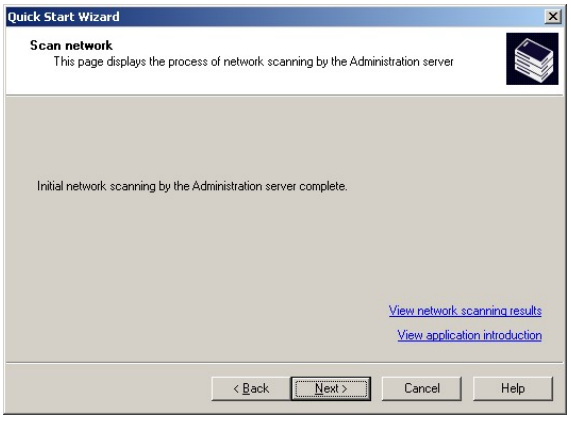


The only minor flaw here is: They could have incorporated a summary in the installation wizard. But now, that is more of an optical deficiency.

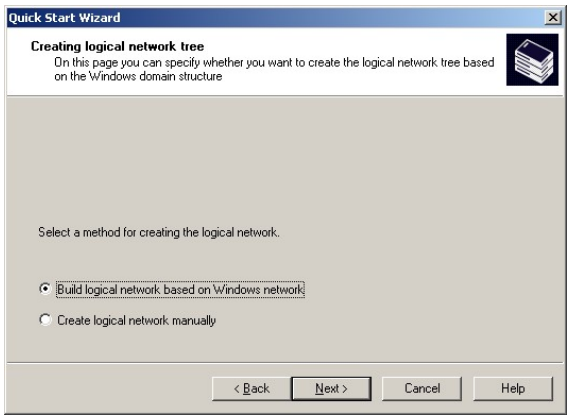
You can now see the Kaspersky menu option in the startup menu. You start the Administration Kit.

As soon as you do this, a wizard appears which then helps you along with the initial steps of the suite.

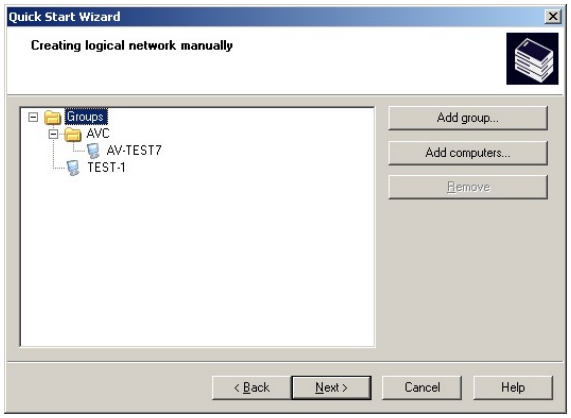
You would naturally accept this help.



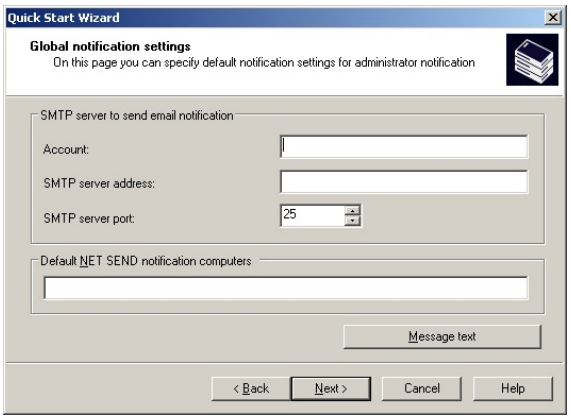
The first thing that the Administration Kit does is to check the network, with which it has to work.

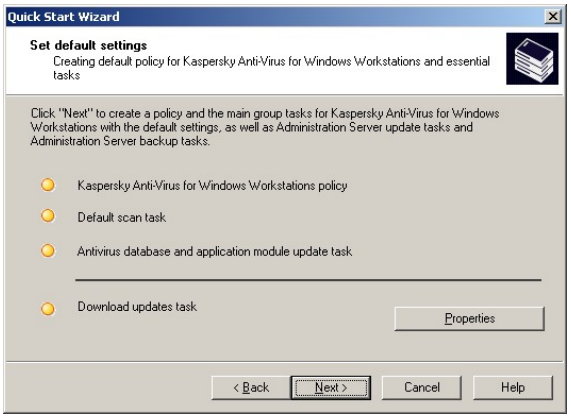


In the next step, the wizard would want to set up the networks with you for the administration. In the case of our test, we select that it should do this based on the Windows network.

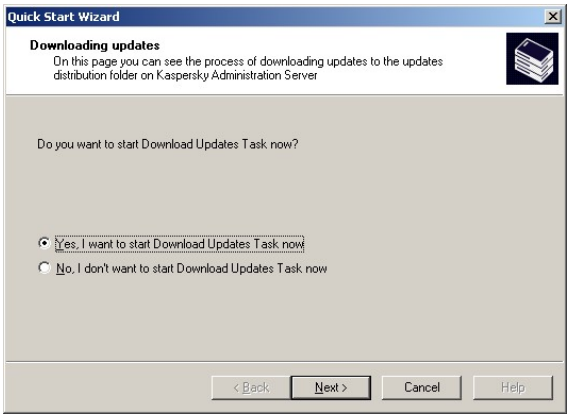


In the next step, you should set up the e-mail address for messages. It is also possible in this case, for the very first time, to send the messages via Net-Send to the Admin. You can also change the message text.

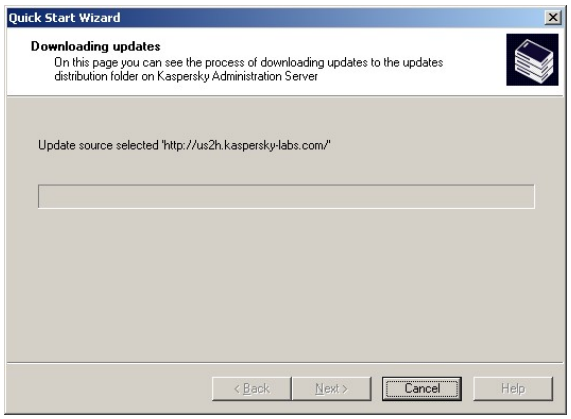




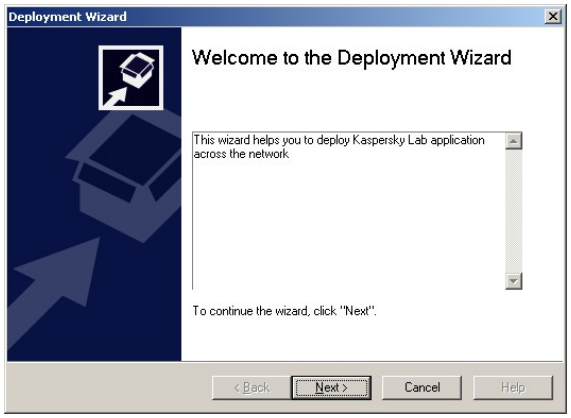
This is where the system explains well and clearly the steps that the Administration Kit would execute next.



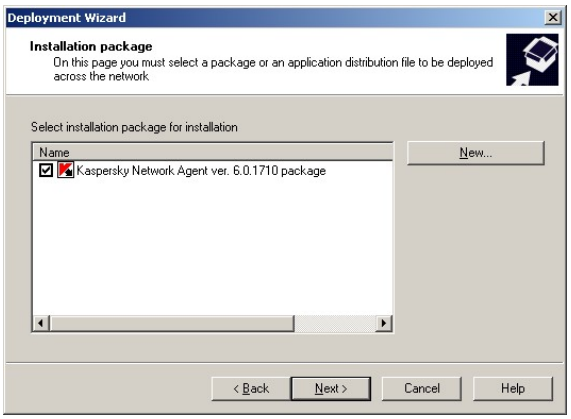
Even here the update task of the Administration Server has been implemented in a very comfortable manner and you can choose between immediate and as per a time schedule.



With this, the first wizard comes to an end and guides you immediately to the next one.

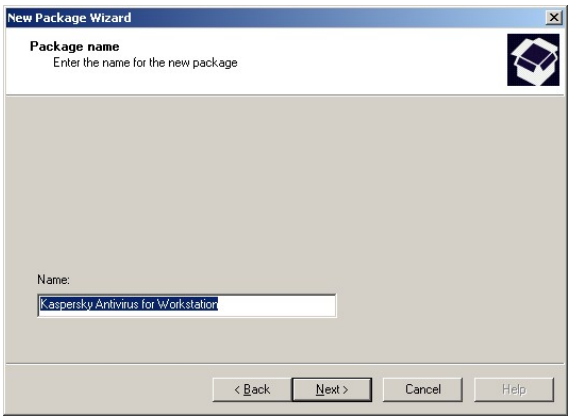


You now continue with the remote installation of the Clients.



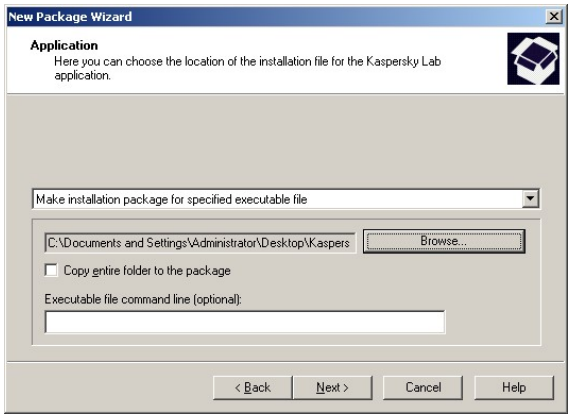
The first action that you have to perform is to install the Agent.

The next step consists of creating the installation package.

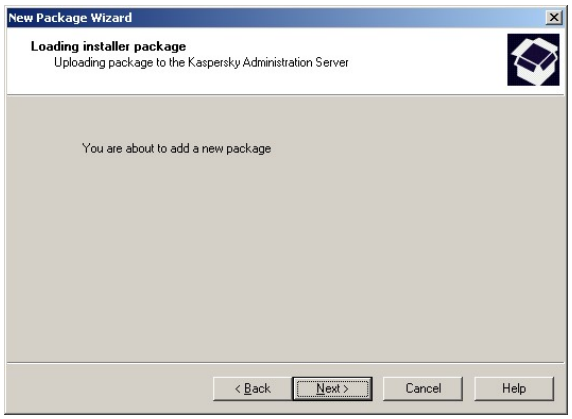


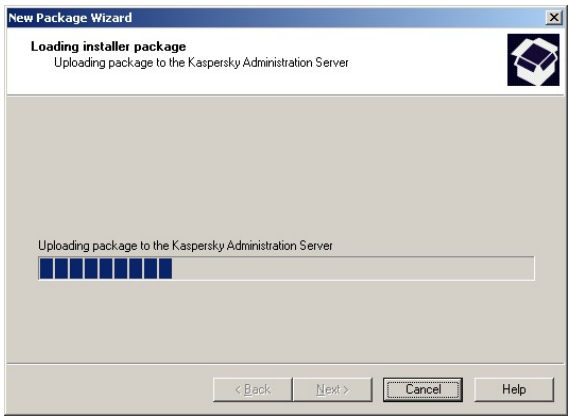
You can select a relevant and meaningful name for the installation kit.

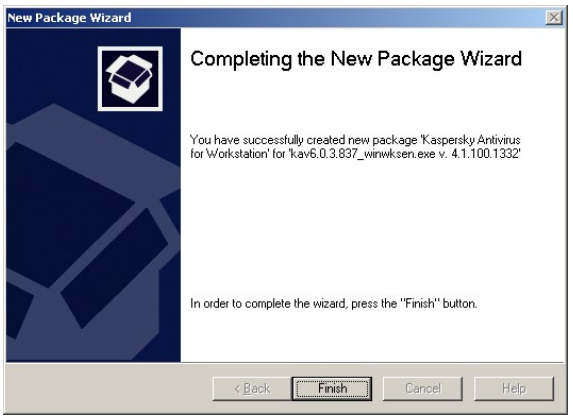
The package is created immediately thereafter.



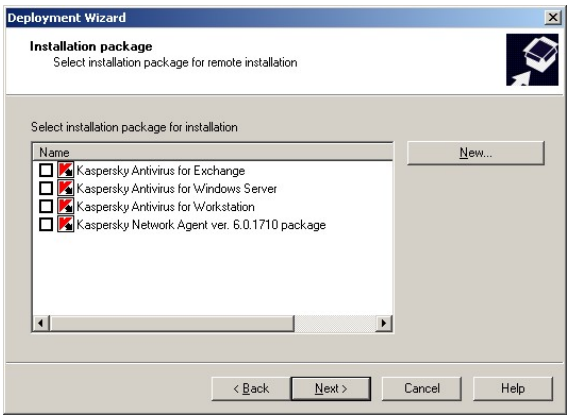
You can select the desired product comfortably using the drop-down list.



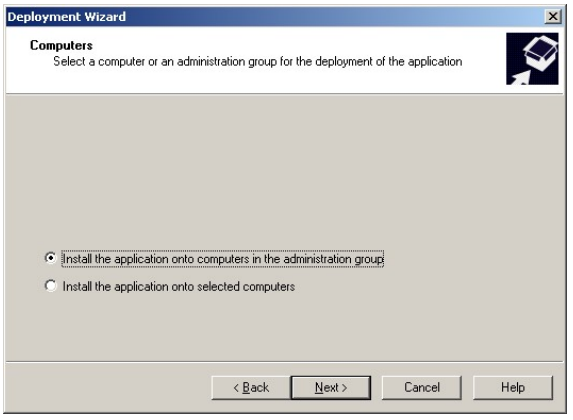


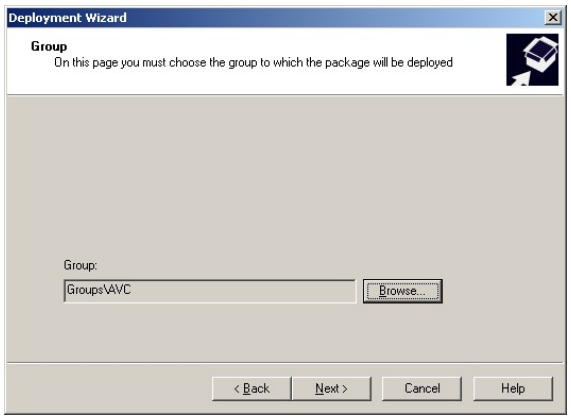


After the installation package has been created successfully, you can proceed with the remote installation.

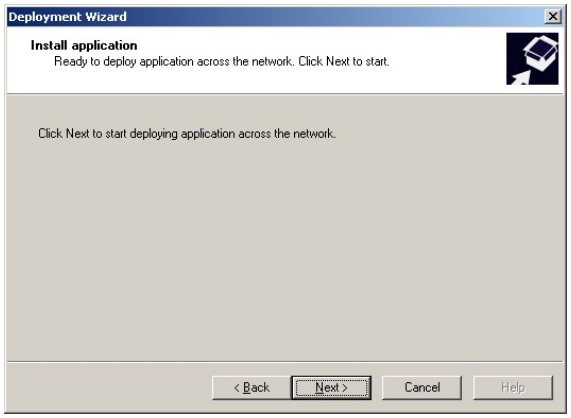


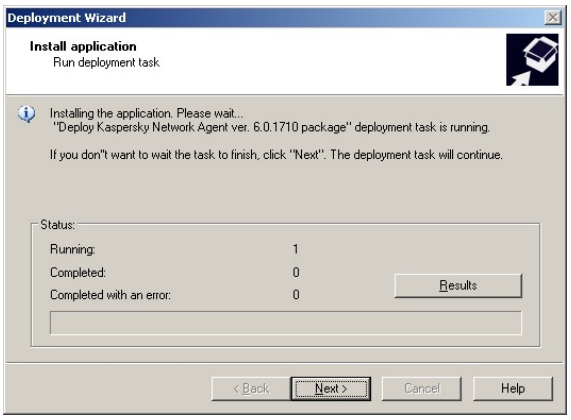
In the next step, you can define groups, for which the installation should be carried out:





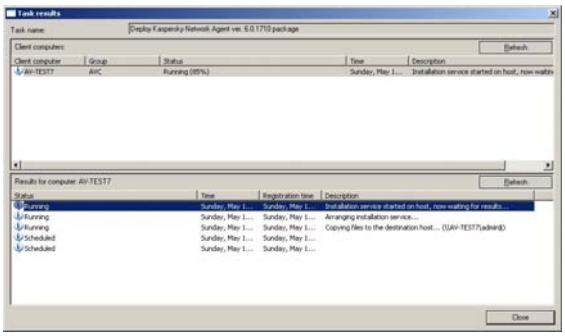
The next step consists of specifying the users, with whom you would like to carry out the remote installation.



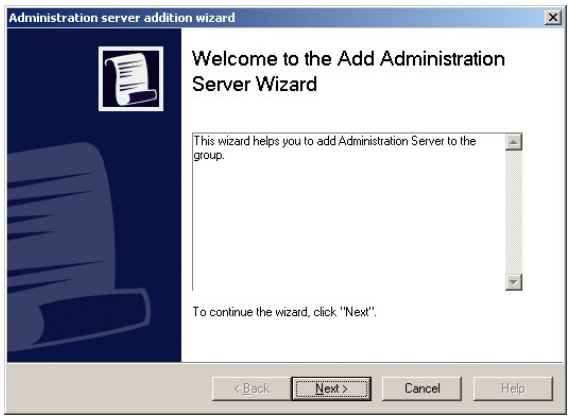


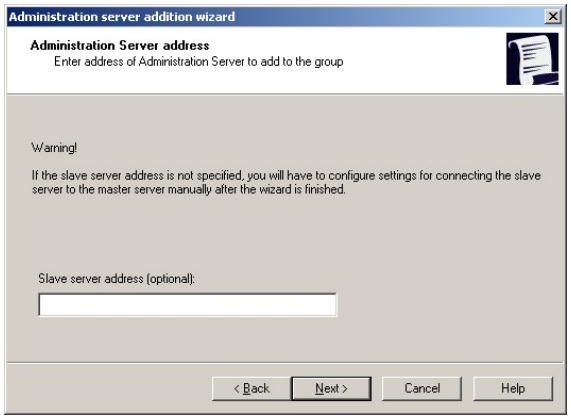
The installation log, as a matter of fact, does not display the status updates in real-time, but with the help of the Refresh button you can have a good overview of what is happening on the remote Client at any given point of time.

The installation runs in the background and you do not have to wait until this Client has been installed, but, instead, you can continue immediately.



In the next step, the installation wizard for the administration server starts up.

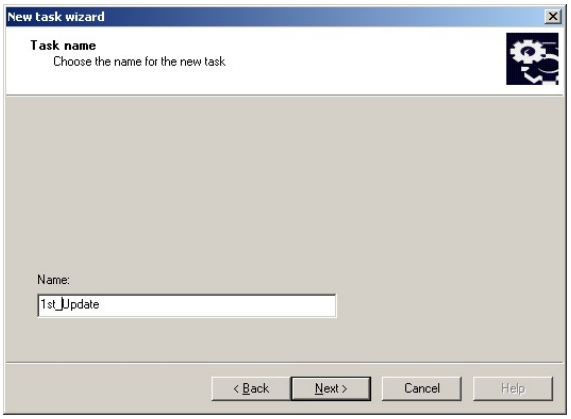




What strikes you here immediately is that the Kaspersky suite is also suitable for large networks having decentralized servers. Since we perform the test with only one server and one client, we bypass the installation at this stage.

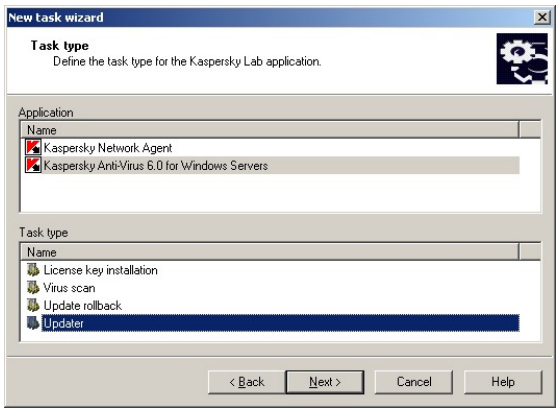
After the installation on the Client and the Server has been completed, the well-designed and structured Administration user interface welcomes you:

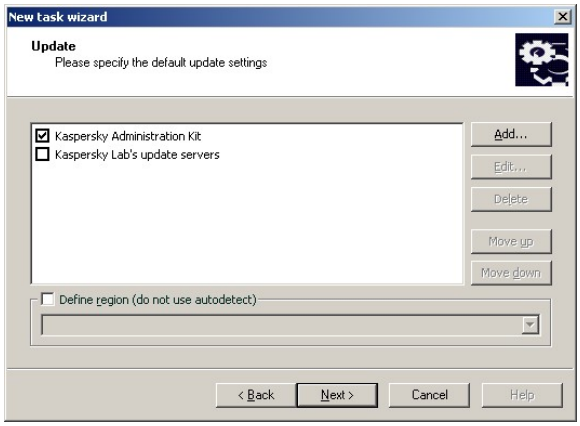
As you can see at first glance, the signatures are naturally not up-to-date, i.e. the first step is to perform an update.



It is a very comfortable feature that you can assign your own names to the various individual tasks. Thus, you do not lose the overview even in large networks.

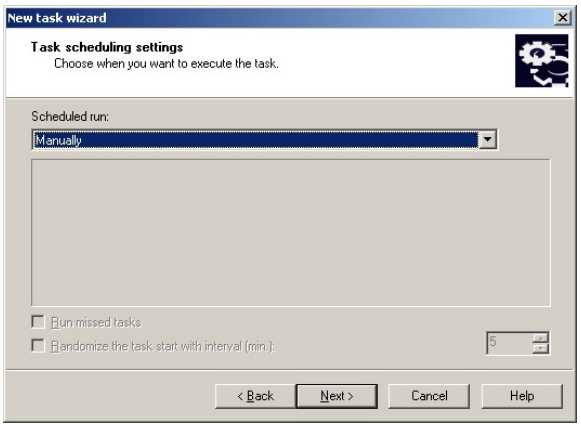
You can select comfortably from among the various tasks specified.



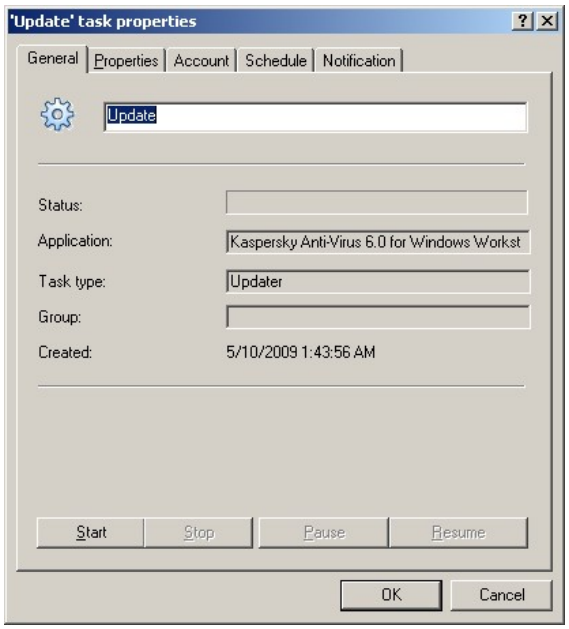


Here, you can also choose the reference source for the signature updates. This is a very comfortable feature.

Even the time schedule can be selected comfortably.



Finally, you can have a detailed look at the tasks once again. The user interface has been adapted to Windows standards and you can find your way around easily and quickly,



Unfortunately, after performing a program update of the server software, it was necessary to restart the server!

However, we must mention that the suite offers a very useful and relevant feature of a rollback for almost all actions.

Summary:

Manufacturer's website (www.kaspersky.com):

The website has been designed elegantly and you can find your way around it quickly. The site complies with the prevalent Internet standards.

You can also order out the products directly from the site and you are not diverted to a local reseller.

This system has its own security zone (threads), in which you can get an overview of the threats from the Internet and also a tip on the product that provides protection against the same.

Over and above this, the site offers removal tools free of charge for current threats. The trial versions of the products are fully functional and run for 30 days.

In addition, the site also offers an on-line virus scanner free of charge.

The Installation Procedure:

The installation of the Kaspersky products is conceivably simple. The installation wizards are very mature and well developed and guide the user through the entire installation procedure.

Moreover, the 4 products tested are also named appropriately and you come to know immediately, without even referring to the manual, which product you need to begin with.

In general, as far as the installation procedure is concerned, you can say that it has been structured neatly and clearly and you need to refer to the manual only in very exceptional cases.

In the process, it must also be mentioned that the system provides excellent Microsoft Active Directory support. The installation wizard configures all the AD-relevant settings. The installation wizard also keeps the user informed in detail about the changes made. Especially with respect to the security structure of the suite, the installation wizard supports the user by reading out the network-related information via the AD.

The suite has optimal default values, which have been aligned perfectly with the needs of a corporate network. If the default settings are not optimal, you can configure the desired settings at the time of installation itself with the help of a few mouse clicks.

The database support provided by the suite is yet another plus point. Kaspersky also supports the open source database MySQL as one of the few manufacturers to do so.

You also have the option of configuring the communication between the individual modules of the suite to meet the desired requirements. You can configure everything easily and comfortably with the help of a few mouse clicks, be it the authorizations between the SQL servers or the ports that should be used for this communication.

The X509 support is another attractive feature, with which the suite is also well

equipped for high-security environments having their own PKI.

The suite sends messages via SMTP or Net-Send.

The update procedure, to be executed the very first time, has also been designed in a very comfortable manner, and even here, you can select whether the first update is to be fetched from an existing Kaspersky server in the network or directly from their website.

The Deployment wizard is one of the greatest strengths of the Kaspersky suite. You can adapt the installation package easily and comfortably, and finally distributed via the wizard, without having to intervene manually with the Clients. The real-time status keeps the user informed and up-to-date regarding the progress being made during the course of installation. You can also have entire groups installed at the same time because of which a large rollout is also no problem and can be handled with just a few steps.

Remote installation executes very quickly on the Clients and the load on the system during the installation is negligible, because of which the user on the Client is not hampered in the course of his work there.

It took us about tow hours to complete the entire installation in our test laboratory including the registration on the website and downloading the products.

The Administrator Console:

You can find your way around the administration console very easily thanks to the MMC conformity. Various menus options have been structured in a manner that is easily understood and self-explanatory.

The menus of the console have been designed in a very simple manner and yet include all functions that are required.

Overall, the console does not leave anything to be desired.

Application Areas:

The Kaspersky suite is suitable for practically all applications thanks to its flexibility and various options for configuring the settings. It is merely in large environments having more than about 1,000 Clients that it can become a little bit complex.

The Admin is kept constantly informed regarding the status of the system and can react quickly and easily to the changing requirements as a result of the good AD support and logging facility.

AV Clients:

Unfortunately, it is necessary to restart the Clients after completing the installation on them.

The message pop-ups are not an eye-sore. After installing the product successfully and starting it, the system executes all the steps necessary automatically.

The user can configure only the most important settings with the least of user privileges.

The Client has also been designed elegantly and appealingly and you can find your way around it almost immediately. The user learns about the status of the system on the summary site.

Conclusion:

The entire suite is very mature and well developed and the wizards have been designed in such a manner that they are very simple and yet comprehensive in their scope.

The logging feature is the best among all products tested by us and the user is always kept well informed about the actions being performed by the suite.

Possibly, you may have desired a summary page in the administrator console, which presents a summary of the status regarding the security system.

Pros and Cons:

+ Good installation wizard having excellent user navigation
+ MS Active Directory Support
+ X509 support
+ Client installation is fast
+ Admin console is designed clearly and coherently
+ Remote installation is very easy
+ Manual is not necessary
+ Good grouping functions are available
+ Also suitable for larger rollouts
+ Support provided for MySQL
+ Good website with an on-line scanner available free of charge

- No summary page in the MMC
- Clients must be restarted after installation
- The first pattern update takes a long time

Application Areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★★	★★★★★	★★★★★

Installation Wizard	★★★★
User Navigation	★★★★★
Administrator console	★★★★
Default Values	★★★★
MS Active Directory Support	★★★★
Database Support	★★★★★
Remote Installation	★★★★★
Website	★★★★★
Manual	★★★★

SOPHOS

Test Software:

SOPHOS Enterprise Security and Control → It contains all products for the File Server and Administration.

SOPHOS Pure Messages → The product for Mail Server protection.

Installation Procedure:

Downloading the Products:

You can find your way easily around the website. The products have been well sorted and named clearly and coherently.

Using a 1.38 MB/sec. connection, the download times were as follows:

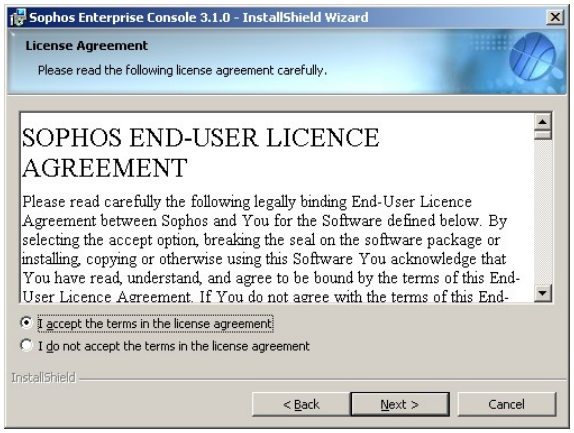
es31sfx (74.8 MB) ⟹ 01:05 min.

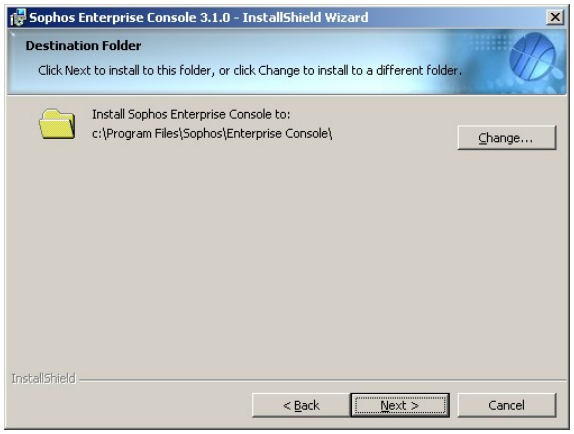
nac312sfx (48.6 MB) ⟹ 34 seconds

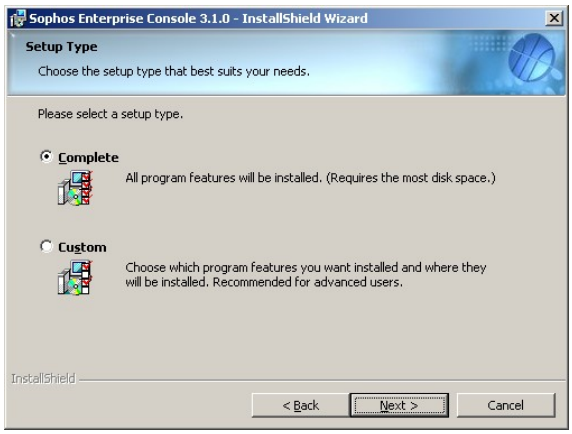
Installing the Products:

You begin with the installation of the SOPHOS Enterprise Security and Control.

The first step consists of unpacking the archive containing the program files.

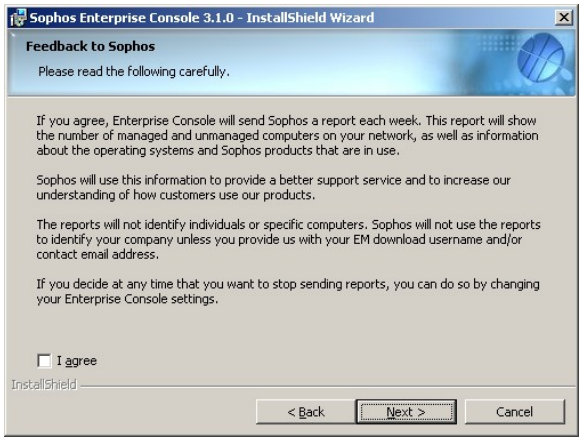




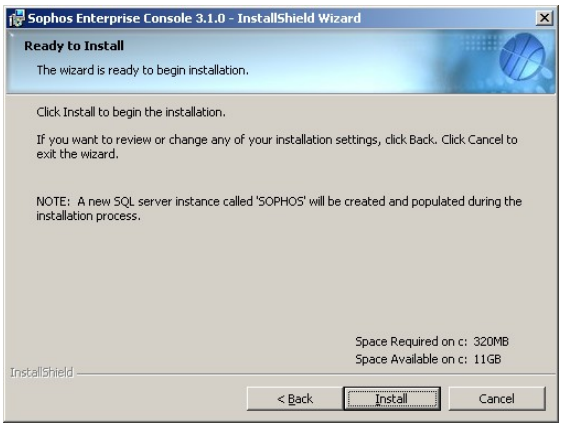


You respond to the standard queries of the installation wizard in the usual manner.

We used the Complete option for installation for the purpose of our test.

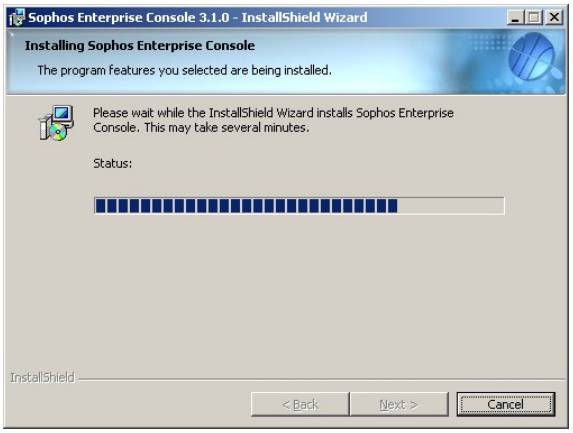


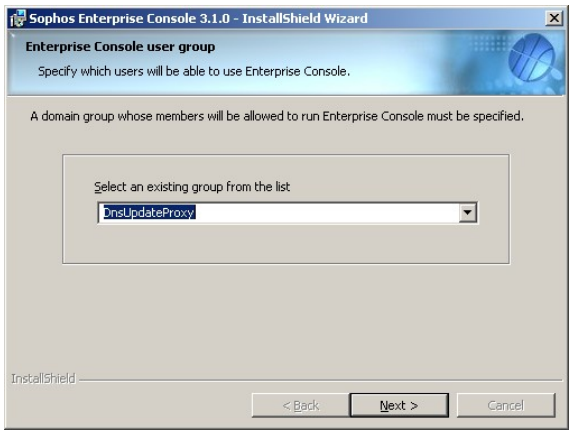
This menu asks if a report should be sent to SOPHOS. We personally, would never enable such a setting option, unless we can see exactly what is being sent to the manufacturer.



The system indicates that a new SQL entity is being created. You do not know which SQL server is being referred to at this stage.

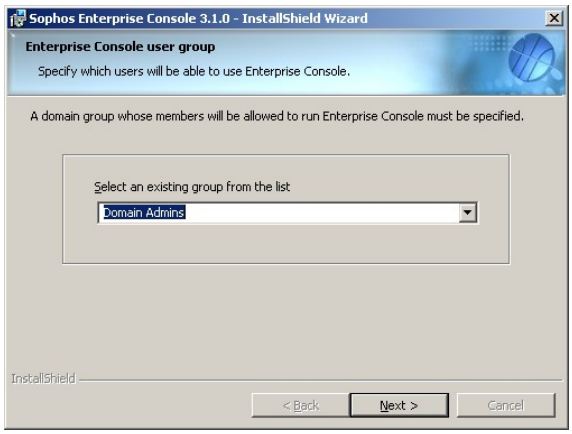
Only after confirming, you know that it refers to the desktop variant of the MS SQL Server.





This is where SOPHOS' focus on the corporate market is clear. The SOPHOS suite offers, by far, the best MS AD support amongst all the products tested by us. You can clearly notice the SOPHOS has the expertise for corporate networks at the time of installing the suite.

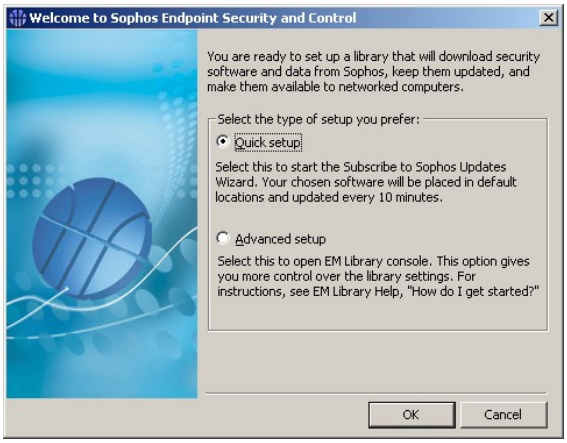
Here, you are asked for the domain group, which should have the privileges for installing and configuring the clients. The "DnsUpdateProxy" group is the default setting for this purpose.



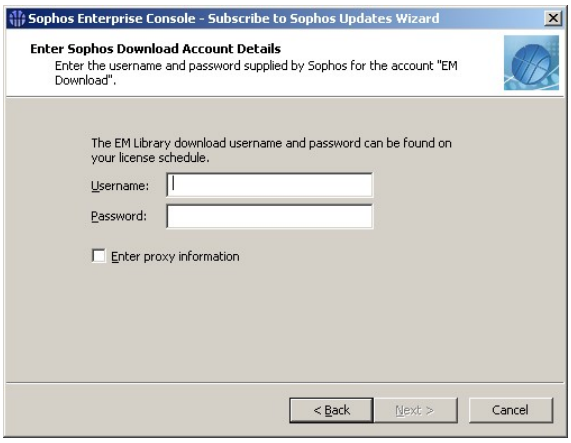
We have selected the domain Admin group for the purpose of simplified installation.

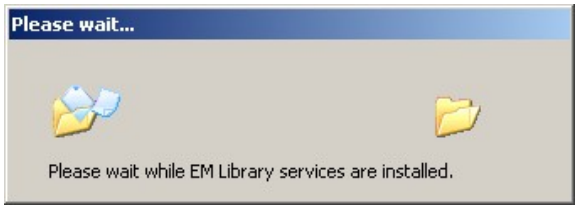
It is adequate to log off and log on to start up the SOPHOS services. You need to be careful only with special Server programs, which require that you are logged in to the Server. This must then, possibly, be started manually.

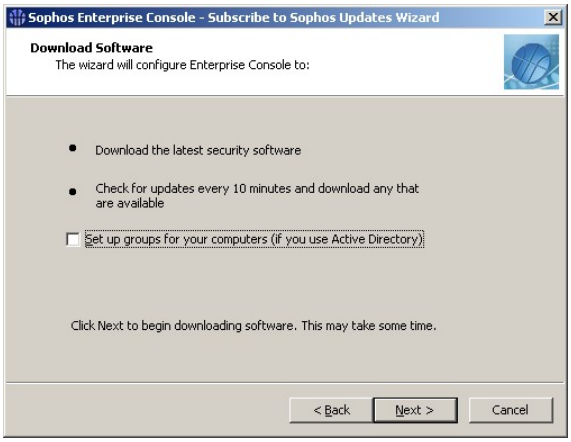
The configuration wizard appears immediately after you have completed the installation successfully, which guides you through the first few steps of the configuration procedure.



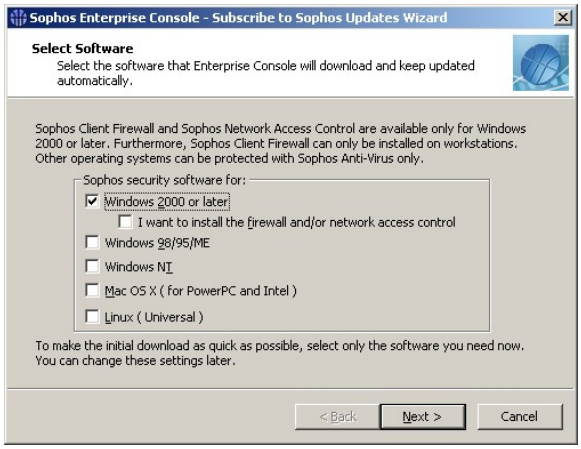
In the first step, you have to specify the update method. The default setting of "10 minutes" for the update interval is appealing here.



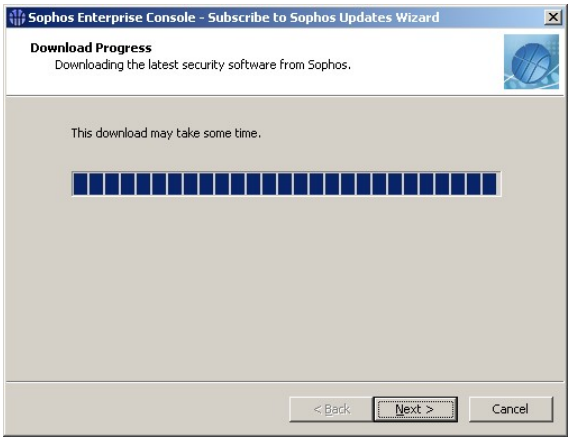




In the next step, the libraries are created.



The following contains a brief summary of the update settings.

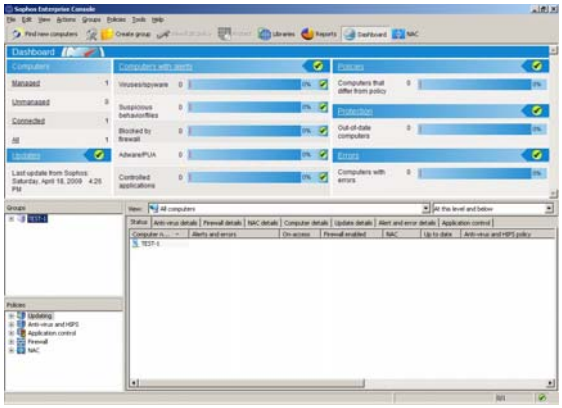


The SOPHOS suite works comfortably even in multi-platform networks.

You need to configure the registration data for the SOPHOS update service here.

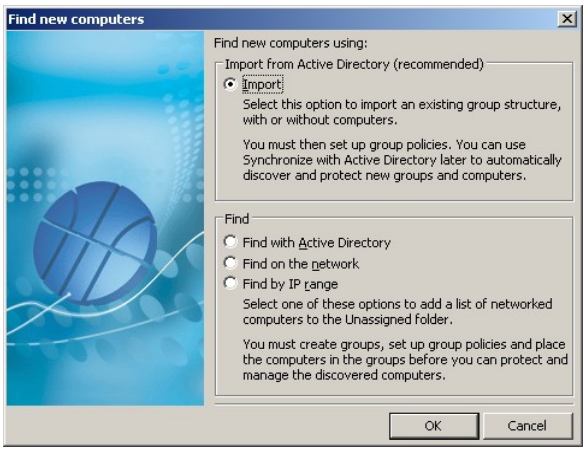
After the wizard has completed, the system enquires about the next steps and if you would like to have more information regarding the configuration.

The Management user interface looks as follows after starting the Manager:

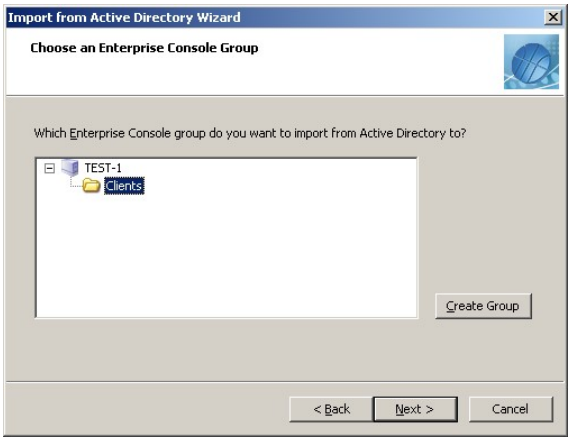


Here too, we have a good example what a comfortable and user-friendly user interface having a summary page looks like.

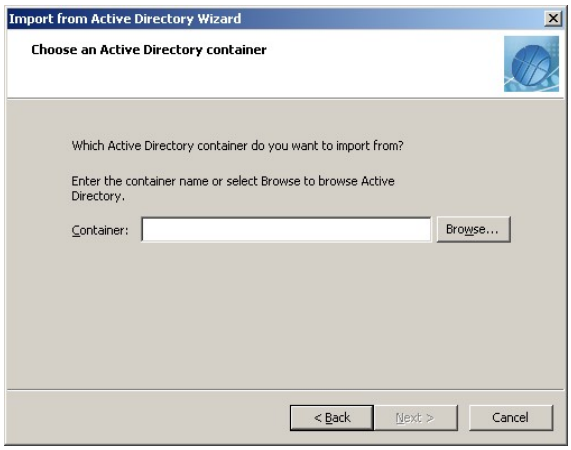
You can import the Clients in the next step. You have the maximum number of methods here for selecting the network computer.

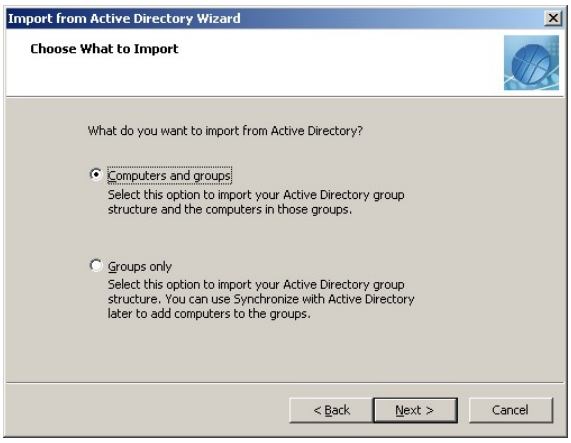


We have selected the Active Directory method.

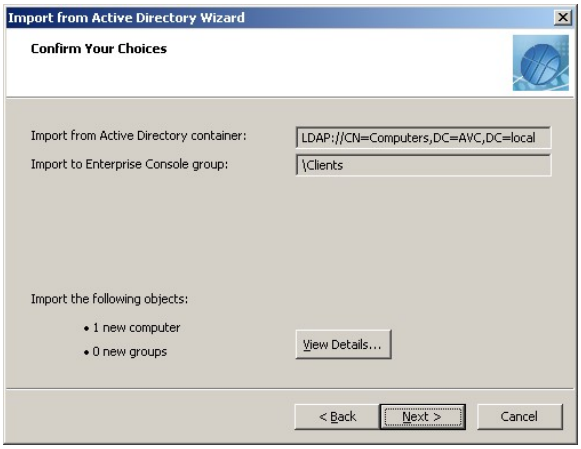


You select the target group next.

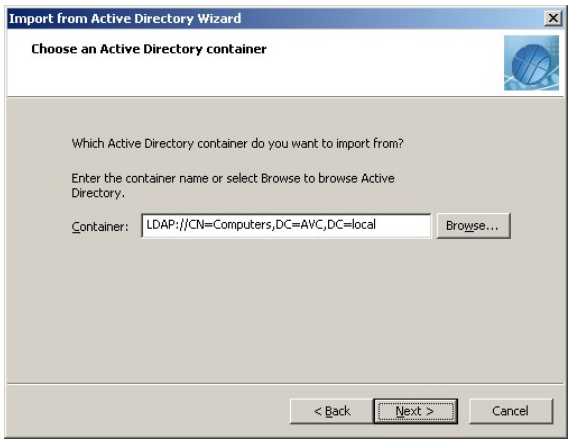




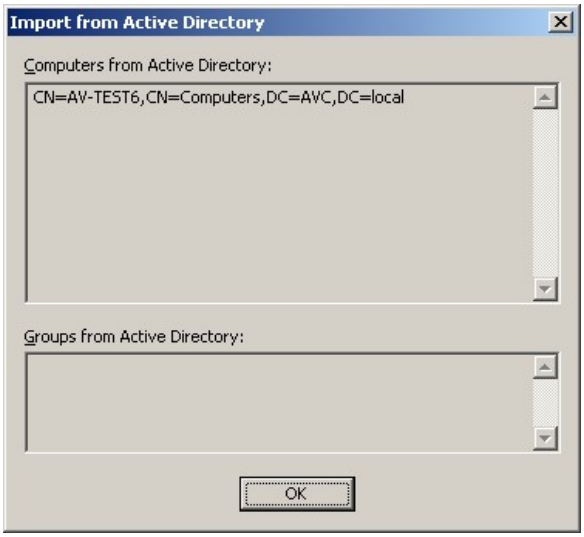
You get to see the excellent support for MS AD here once again.

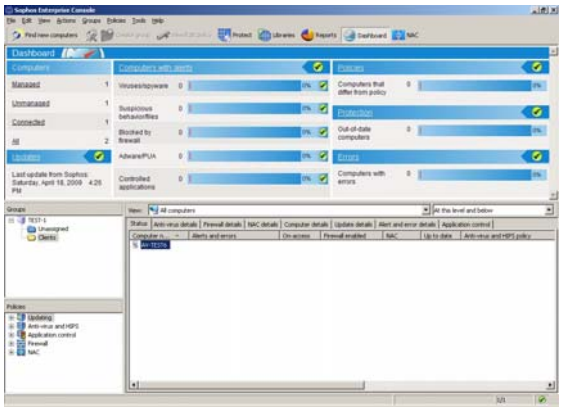


The Clients are also optimized after presenting a brief summary. As a result of this procedure, it is also possible to import a very large number of clients in very large environments.



The system displays the Container and the Object in LDAP-compliant URI.

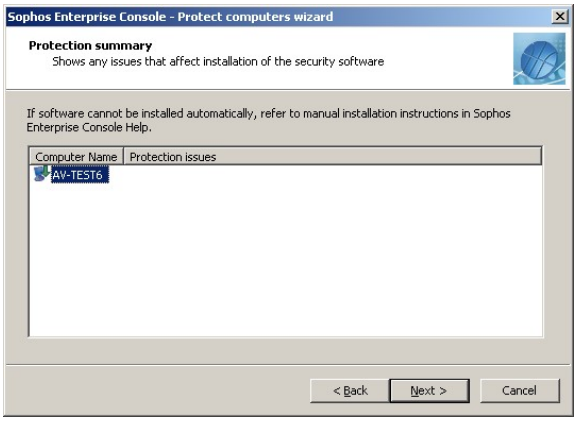


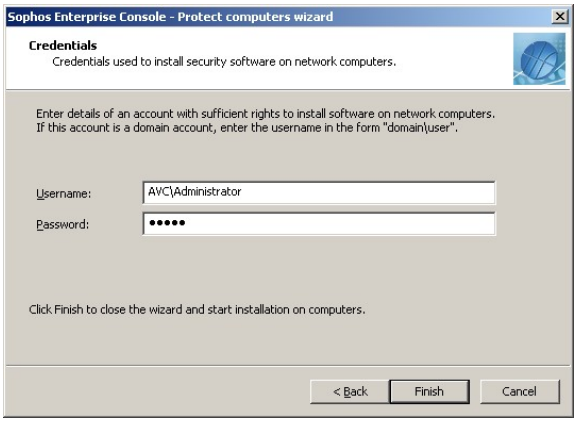


You can now view the Clients that have been imported in the groups to which they have already been assigned previously.

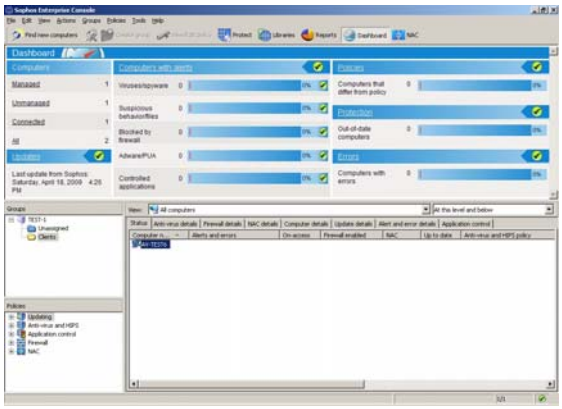
In the next step, the wizard for installing the Client software starts up on the systems.

This system also has the unique setting, which permits the un-installation of the security software of other manufacturers.





These are the settings of the account for installing the software on the systems.



After the installation has been completed, the Client is incorporated in the overview of the management console.

Summary:

Manufacturer's website (www.sophos.com):

The website is appealing and has been structured clearly. The site complies with the prevalent Internet standards.

The website itself gives you a clear overview of the current threats. It is possible to subscribe to various RSS news so that you are always kept up-to-date with the latest events.

Over and above this, the site offers removal tools free of charge for current threats.

The trial versions of the products are fully functional and run for 30 days.

The Installation Procedure:

The installation of the Sophos suite is extremely simple and has been designed in a structured manner. The wizards have been designed in a very simple manner and provide all the setting options required.

Moreover, the three products tested are also named appropriately and you come to know immediately, without even referring to the manual, which product you need to begin with.

The SOPHOS suite offers, by a long shot, the best MS AD support amongst all the products tested by us. You can see from the installation wizard itself that Sophos offers only corporate products. The entire suite is perfectly designed to meet the needs of corporate environments.

The user realizes immediately that he can also install thousands of Clients with just a few mouse clicks using the wizards provided.

What is disappointing, however, is that the system has been somewhat conservative with the database support and it has implemented support merely for the MS SQL desktop engine supplied along with the system. It would have been nice if you could have selected the database yourself.

You can configure various settings for authorization during the installation procedure itself. You can navigate easily and comfortably in the AD to the desired groups / users, which you would like to administer for various tasks. As a result, the system also provides support for a multi-Admin environment.

You also have the option of sending a weekly report to Sophos. However, Sophos has not configured this option as the default setting.

After the installation is complete, it suffices to log off and log on to the system in order to enable the services.

After logging on to the server again, the endpoint protection wizard appears on the screen. After installing the client software, the system enquires immediately about the first update. This then takes the better part of about 20 minutes. By default, the system picks up subsequent updates for the Clients directly from the server.

During the first update procedure, you can select the Clients that should be updated using the AD.

Thanks to the wizards provided, installing the suite is very simple and goes like a breeze.

The remote installation of the Clients has been implemented very well. As a result of the perfect AD support, you have the option to carry out the remote installation via AD objects also. Installation of the remote Clients executes very quickly.

The Administrator Console:

The Sophos Enterprise console is the first one in our test, which provides a good overview on the summary site about the status of the security system.

The console, in itself, has been well structured, and you can find your way around it very quickly. It is not inconvenient or uncomfortable, even if you select a structure that is somewhat different from the standard views of the MMC.

The great strengths of the console are definitely the options provided for filtering and grouping. It is possible, without putting in any extra effort, to administer a very large number of Clients, thanks to the AD support. Hence, you do not need to set up your own groups, but, instead, you can use the grouping of the MS AD already available.

The most important functions are arranged in the form of a taskbar and thus, facilitate navigation within the console.

Application Areas:

The Sophos suite, with its mechanisms, is the optimal choice for all kinds of networks. Although you can reap the benefits provided by the suite only in medium to large-sized networks, it is also not a problem to deploy it on small networks to cover all the needs and requirements.

It is possible to administer environments having more than 100000 users due the excellent options provided by the system for filtering and grouping.

You can implement larger rollouts easily and quickly as a result of the database support and the perfect AD support provided.

AV Clients:

The message pop-ups are not an eye-sore. After installing the product successfully and starting it, the system executes all the steps necessary automatically.

The user can control all functions necessary with the bare minimum of authorization settings, without having too many privileges, which could lead to incorrect changes.

The user interface has been designed elegantly and you can find your way around it easily.

Conclusion:

SOPHOS has, by a long shot, the best AD support amongst all products tested by us. You notice with the entire structure that SOPHOS offers only corporate solutions in its range of products.

The great strength of this suite lies in the fact that even large rollouts can be executed with a bare minimum of administrative effort. It is, thus, possible, to install many thousands of Clients with the help of just a few clicks of the mouse.

Overall, it is a very mature and professional solution, which has been conceived for practically all sizes of networks, and the strengths really come into focus particularly with networks having more than 500 systems.

The only point with respect to the database support provided is that it would have been nice if open-source databases such as, e.g. MySQL had also been supported.

In high-security environments you must carefully consider the optional report to SOPHOS.

Pros and Cons:

+ Good installation wizard having excellent user navigation
+ The best MS Active Directory Support
+ Client installation is fast
+ Admin console is designed clearly and coherently
+ Remote installation is very easy
+ Reading the manual is not necessary
+ Good grouping functions are available
+ Good filter options are provided
+ Summary site in the Admin console
+ Also suitable for larger rollouts
+ Good website offering removal tools free of charge

- Consideration of the report to Sophos is critical in a high-security environment
- fixed selection of database

Application Areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★	★★★★★	★★★★★

Brief Summary:

Installation Wizard	★★★★★
User Navigation	★★★★
Administrator console	★★★★★
Default Values	★★★★
MS Active Directory Support	★★★★★
Database Support	★★★★
Remote Installation	★★★★
Website	★★★★
Manual	★★★★

Symantec

Test Software:

Symantec Endpoint Protection → It includes all products for the File Server, Mail Server and Administration.

Installation Procedure:

Downloading the Products:

Menu navigation provided by the manufacturer has been structured coherently and kept simple. It is easy for the user to find the desired products and it is possible to download all products with their entire scope of functionality even without registration.

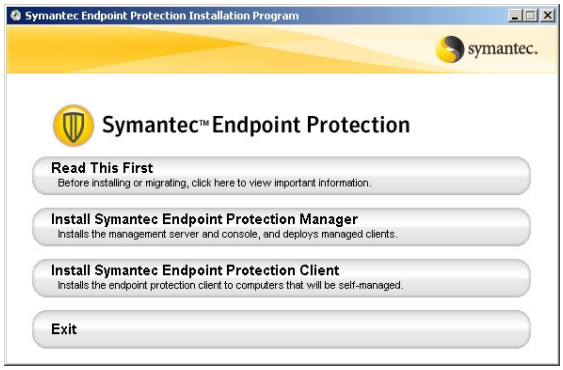
Using a 1.38 MB/sec. connection, the download times were as follows:

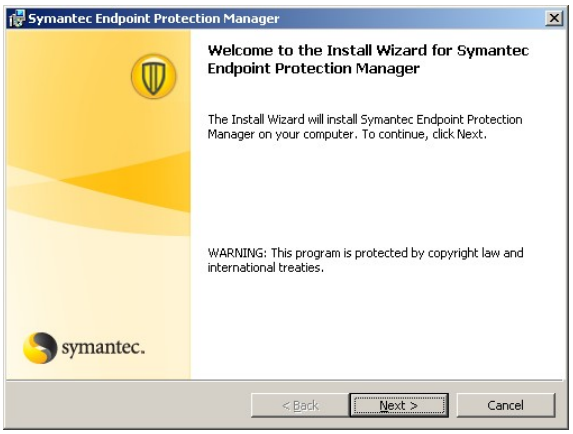
Symantec Endpoint Protection CD 1 (420 MB) ⇒ 04:05 min.

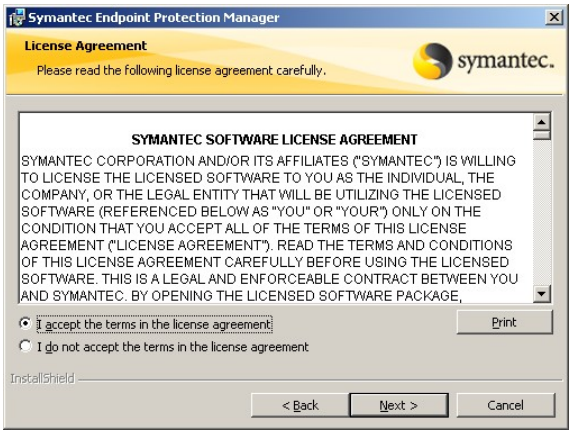
Symantec Endpoint Protection CD 1 (445 MB) ⇒ 04:31 min.

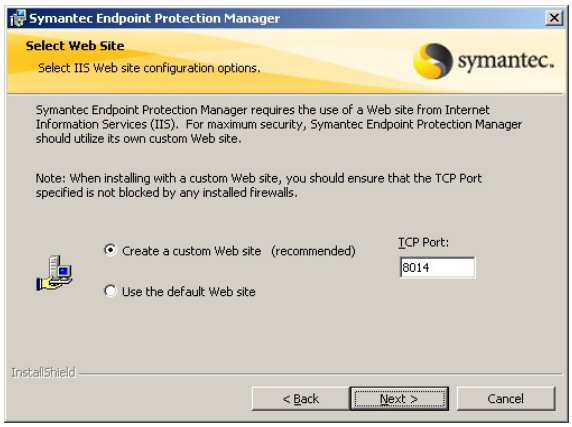
Installing the Products:

You begin by installing the Symantec Endpoint Protection Manager.



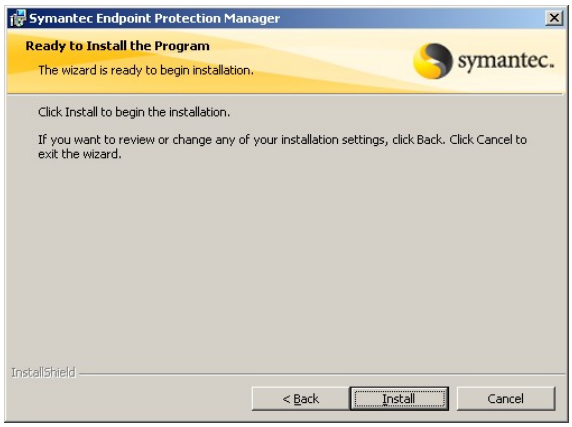


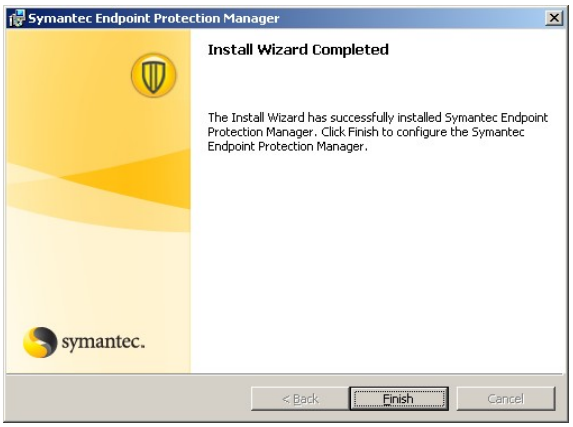




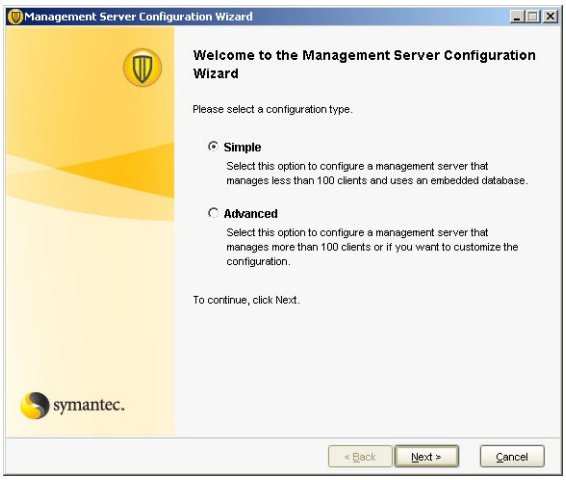
After responding to the standard queries, the next step consists of configuring the IIS required for operating the Management Console.

The system recommends correctly at this stage, that a separate website should be configured for the Manager. You should also comply with this requirement in any case. You should only not forget the FW settings.

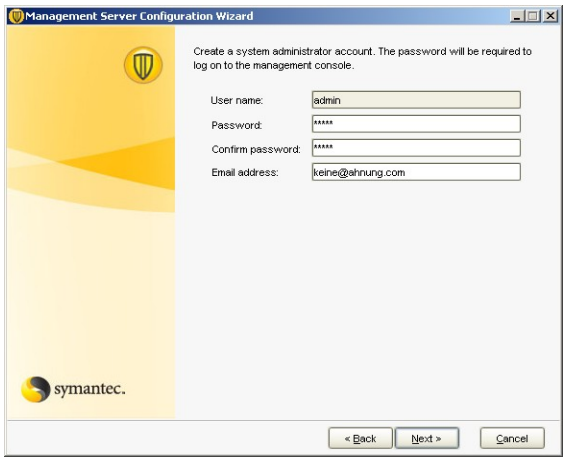




Even in this case, the configuration wizard for the Management Console appears after completing the configuration:

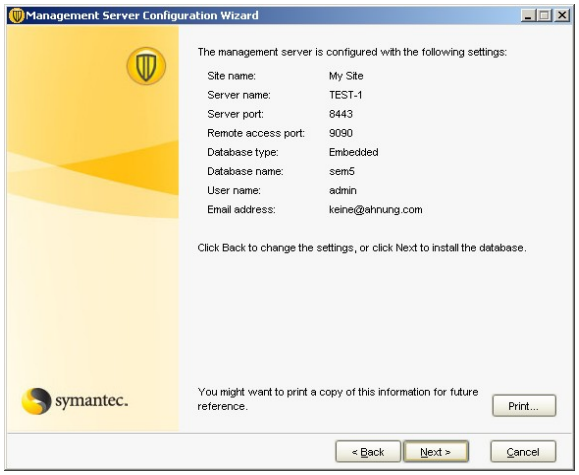


As the first step, you can choose between two different configuration methods. This depends on the environment in which you wish to use the suite. We have used the simple method in our test.



This is where you specify the user for the Management Console. You would have desired to have AD support in this case. You can change it in the User-Interface afterwards.

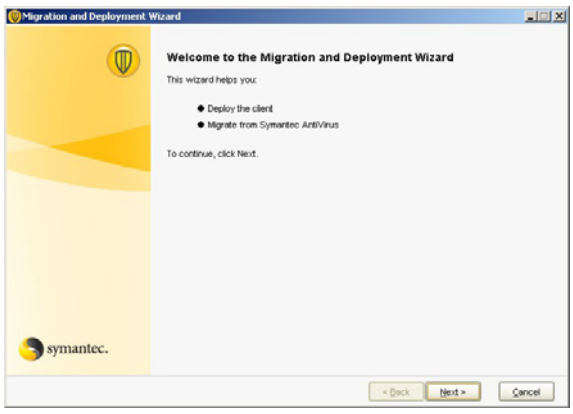
A positive aspect to be noted here is that the password must comply with the complexity requirements.

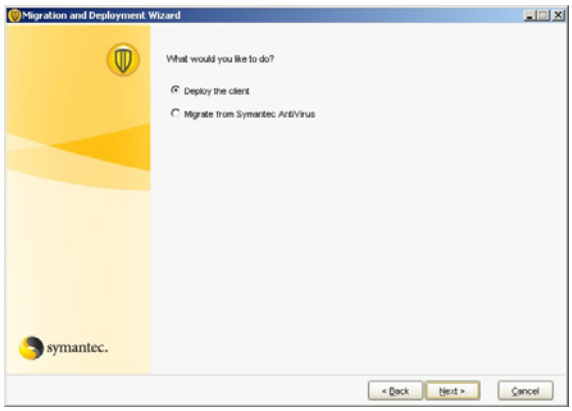


What is very convenient for an Admin having good documentation is the option that the configuration settings for the IIS can be printed out.

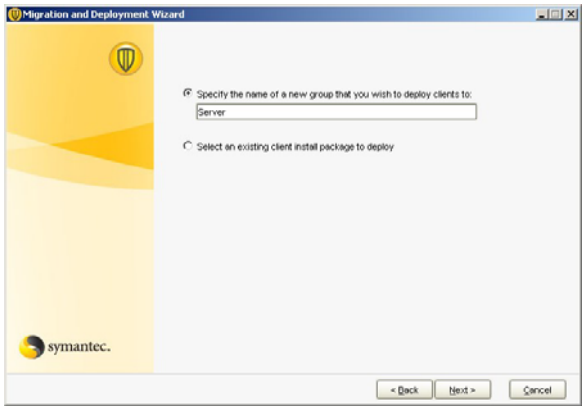
This window keeps you waiting for the maximum period of time during the course of the installation. The wizard required an unbelievable 25 minutes to create and initialize the databases.

After you cross this hurdle of patience, the configuration of the Management Server is complete and you can continue with the installation wizards for the Clients.

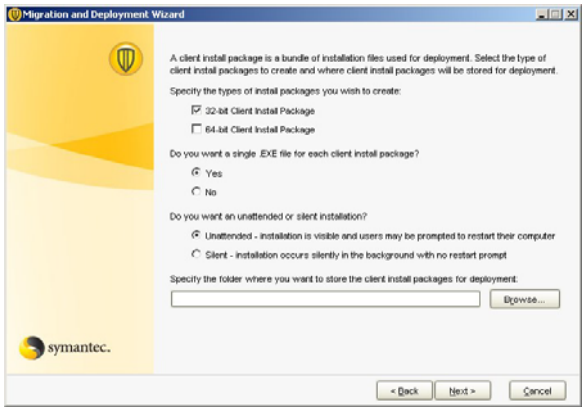




You have the option here to migrate the existing antivirus Clients.

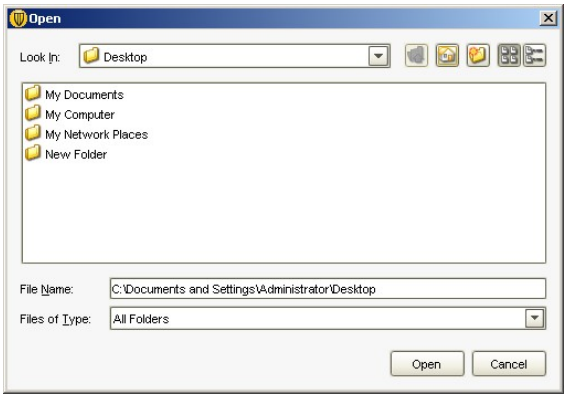


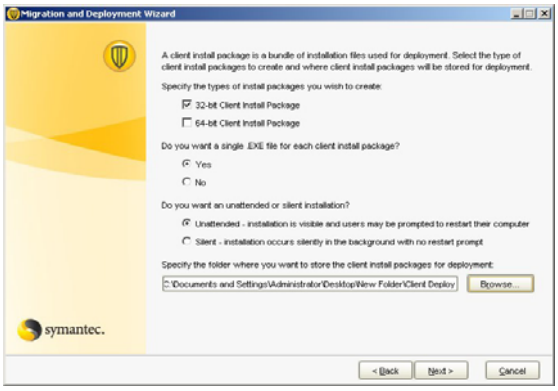
Here, too, you can divide the Clients and Servers in groups.



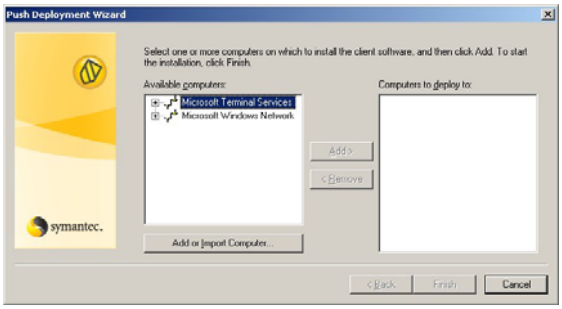
You can select the desired variant conveniently with the settings for the Client installations.

You can define the network share easily with the help of a browser button. This is how it should be!



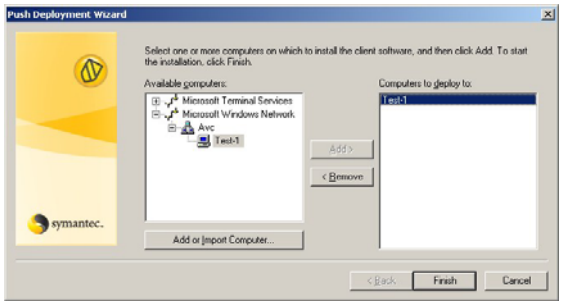


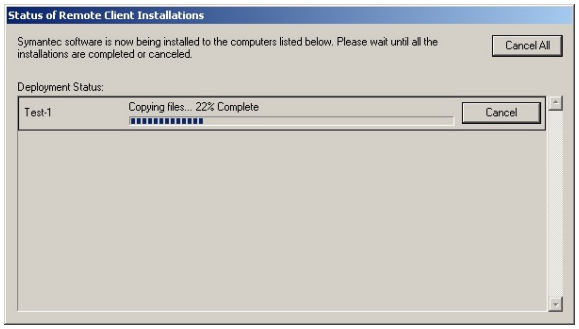
After completing the configuration, the required Client packages are created.



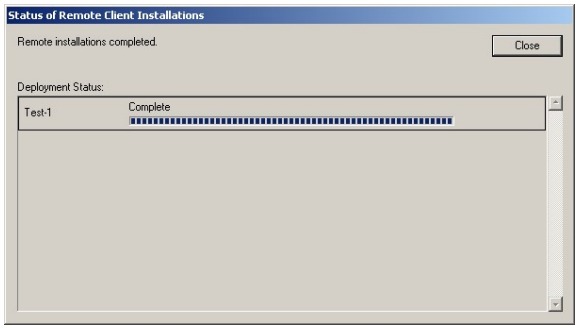
You can now conveniently select the systems via this network window.

You can specify the login data for each Client separately.



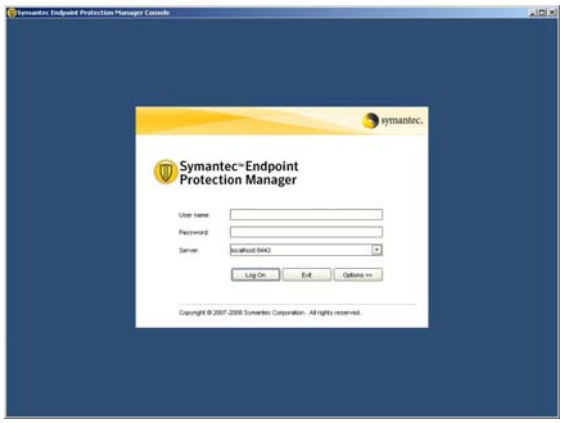


You can also see the real-time status messages regarding the installation of the Clients.

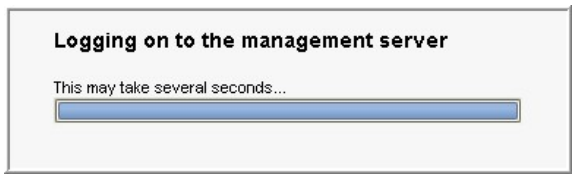


After the Clients have been installed successfully, they execute an update immediately. It would have been desirable here if you could have the choice to specify whether you would like to update or not.

Unfortunately, in this case too, system restart is necessary. The reboot of the client is required to enable the firewall, application and device control and network IPS functionality. For these technologies to work it has to register drivers which requires a reboot. The Antivirus and anti-spyware modules are active and provide protection immediately after the installation.



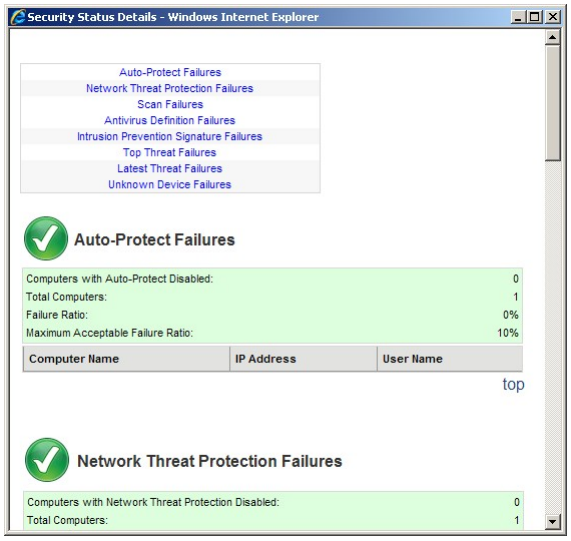
This window appears after invoking the Manager.



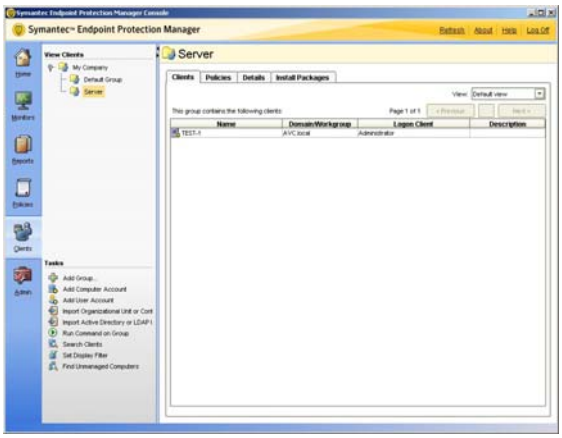
This is what a summary page should look like. You get an instantaneous overview about the status of the entire Symantec environment.

The Manager has been designed very elegantly and attractively both logically and optically. Even in this case, it is as good as not possible to have real-time logging via the web user interface.

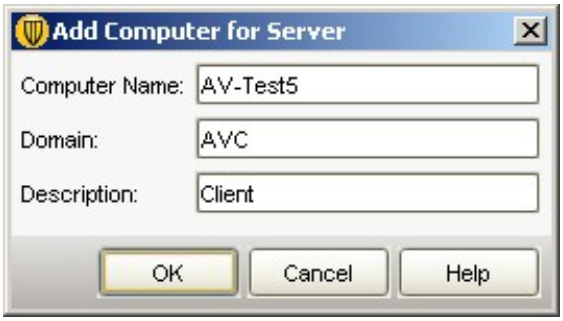
You have a detailed overview of the status of the Clients.

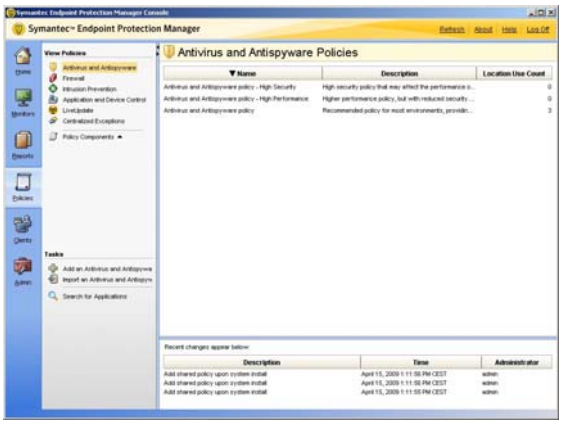


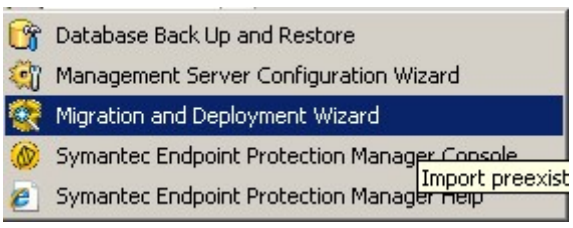
The user interface leaves nothing to be desired with respect to the operation and division of the environment.

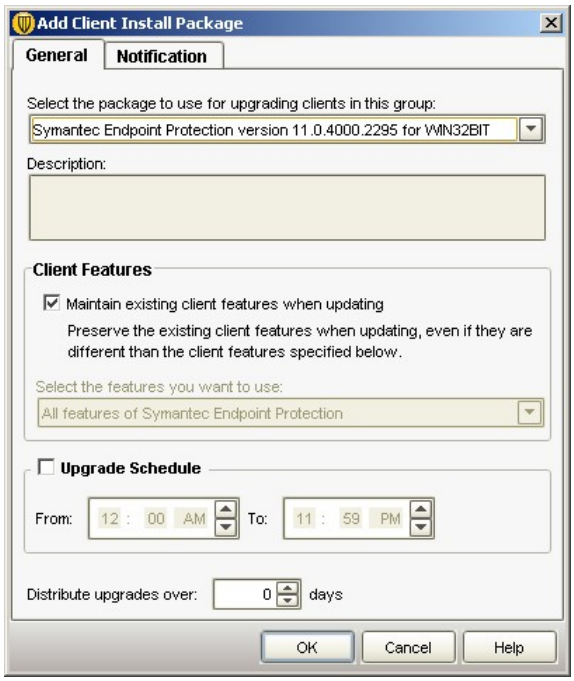


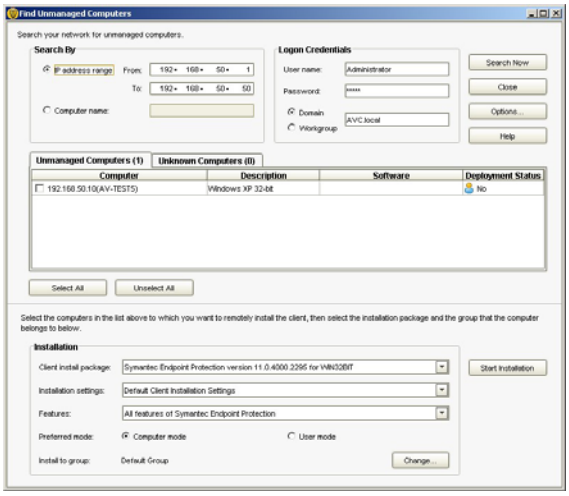
All topics and actions have been described well and are self-explanatory. You definitely do not need a manual in this case.



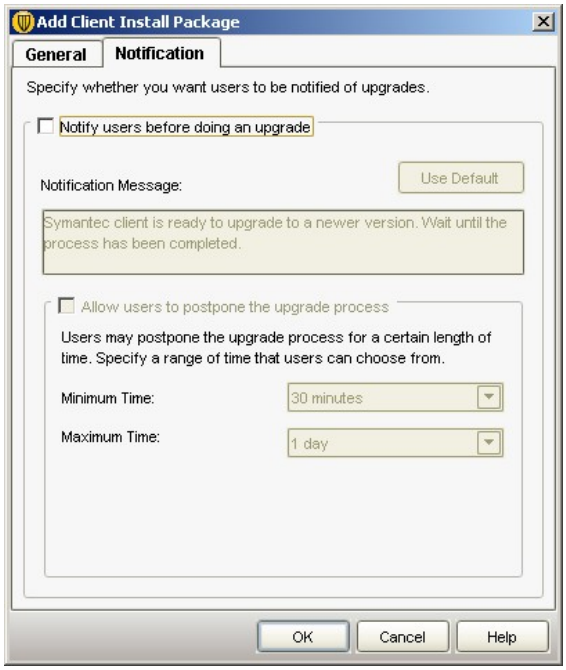


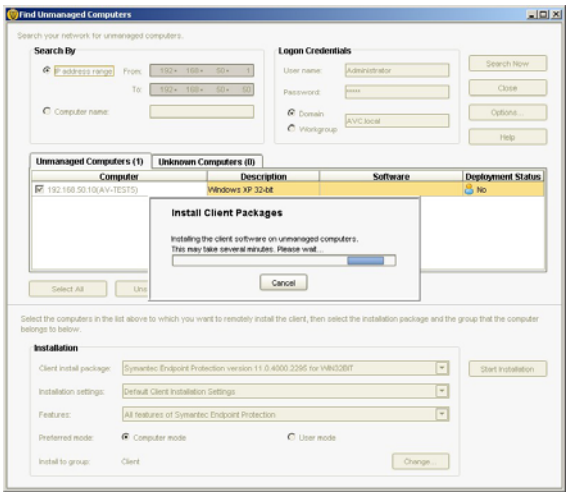


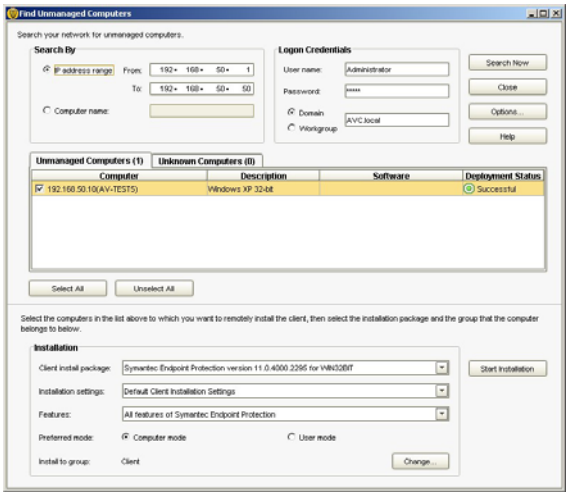




Even the installation wizard has been designed perfectly.







Summary:

Manufacturer's website (www.symantec.com):

The website is appealing and has been structured clearly. The site complies with the prevalent Internet standards.

The website itself gives you a clear overview of the current threats.

Over and above this, the site offers removal tools free of charge for current threats.

The trial versions of the products are fully functional and run for 30 days.

In addition, the site also offers an on-line virus scanner free of charge.

The Installation Procedure:

The user can see that Symantec has acquired adequate experience over the years starting with the installation wizard itself. Thus, you are guided by a perfectly designed installation wizard through the entire installation procedure.

As the first step, the IIS must be installed in case it is not yet available, since the Management Console uses a web user interface.

You need only one installation wizard to install the suite, which, in turn guides you to the two products tested by us.

Even the configuration of the IIS (Internet Information Server) is very simple in design, thanks to the excellent installation wizard.

The two configuration options provided by the installation wizard are very appealing and attractive. The user can choose between "Simple" and "Advanced". Depending on the size of the environment, you can select the desired configuration variant.

The "Simple" configuration has been conceived for networks having up to 100 Clients and the "Advanced" variant is meant for more than 100 Clients.

In the case of the simple method, you only have the option to create one single Admin account for the Administration Console.

Here again, you notice the quality of the product since the password must comply with the complexity requirements.

Even the option of being able to print out a summary of the settings as a document is a very nice feature.

What is striking is the extremely long time that the suite needs to create the databases. We needed more than 25 minutes in our test environment before we could continue.

Even in the case of Symantec, you are guided to the next wizard after the previous one has completed its task. In our case, it was the "Migration and Deployment Wizard".

Here, you have the choice of integrating either new Clients or existing Symantec Clients into the corporate suite.

The configuration options for the Deploy are diverse and versatile and do not miss out on any important setting. This is the first time that you can create the packages selectively for 32-bit or 64-bit systems.

The status information of the remote installation is, in fact, not very detailed, but, nonetheless, in real time. Even in the case of this suite, it is not necessary to undertake cumbersome preparatory work on the Clients or in the environment.
Unfortunately, it is necessary to restart the Server after completing the installation on the Clients.

The Administrator Console:

After logging in to the Admin console, you have, by far, the best summary site appearing as compared to all the products tested by us. This is where the other manufacturers could take a leaf out of their book!

The admin console was one of the easiest consoles to administer in the tests carried out by us. It is well designed particularly from the graphical point of view and the most important functions can be seen at a glance.

The Symantec admin console is extremely advanced and well developed in every aspect and leaves nothing to be desired.

AV Clients:

Here too, the manufacturer's know how is ubiquitous. There is no function that you miss out on and the Client in our environment is very lean in design and does not consume too many system resources.

The live update executes immediately after the Client deployment. This is where you could have desired yet another configuration option to start the update manually or to specify the path for the update yourself.

The user can control all functions necessary with the bare minimum of authorization settings, without having too many privileges, which could lead to incorrect changes.

Application Areas:

As already described under the "Installation Procedure", the suite is suitable for practically all sizes of the environment.

You are always well advised with the Symantec suite regardless of whether it is a rollout for many thousands of clients or you merely want to protect a small network having 5 users.

Conclusion:

The Symantec suite is, by far, the most mature and professional product tested by us. At every step, you notice the extensive experience on the part of the manufacturer in the security and antivirus environment.

The only negative point is the long time required for the installation.

Pros and Cons:

+ Very good installation wizard having excellent user navigation
+ Client installation is fast
+ Admin console is designed clearly and coherently
+ Remote installation is very easy
+ Manual is not necessary
+ Good grouping functions are available
+ It has the best summary site in the Admin console
+ Also suitable for larger rollouts
+ Very good website offering removal tools free of charge

- Very long time required for the installation of the Management Console

Application Areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★★	★★★★★	★★★★★

Brief Summary:

Installation Wizard	★★★★
User Navigation	★★★★★
Administrator console	★★★★★
Default Values	★★★
MS Active Directory Support	★★★★
Database Support	★★★★
Remote Installation	★★★★★
Website	★★★★★
Manual	★★★★

TrustPort

Test Software:

TrustPort_Management_Server_EN	→	Admin Console
TrustPort_Management_Client_EN	→	Management Agent
TrustPort_Antivirus_Business_EN.exe	→	Anti-VirusProtection

AV comparatives

Installation Procedure:

Downloading the Products:

Menu navigation provided by the manufacturer has been structured coherently and kept simple. It is easy for the user to find the desired products and it is possible to download all products with their entire scope of functionality even without registration.

Registration is required for a test key. Thereafter, 30 days are available to test the desired products extensively. Data is then forwarded to a certified partner of Trustport.

Using a 380 KB/sec. connection, the download times were as follows:

TrustPort_Management_Server_EN
(25.7 MB) ⟹ 01:08 min.

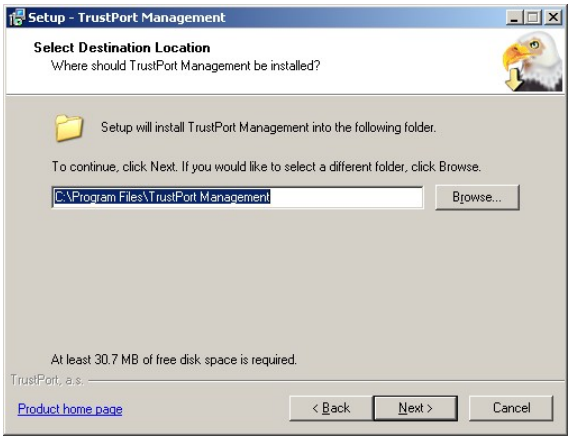
TrustPort_Management_Client_EN
(2.6 MB) ⟹ 7 seconds

TrustPort_Antivirus_Business_EN.exe
(156 MB) ⟹ 08:10 min.

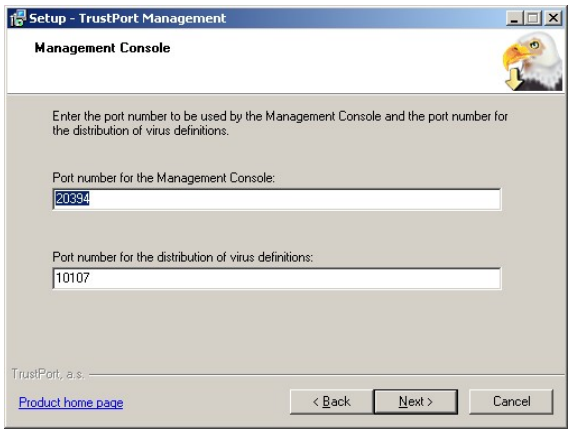
Installing the Products:

It is very convenient here since the names of both the products specify where you have to install them. You begin with the server.

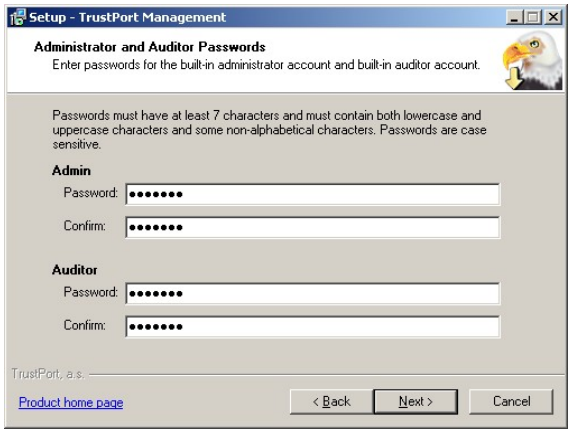
You can commence with the installation after accepting the mandatory queries regarding the license agreement.



In our example, we retain the default path.

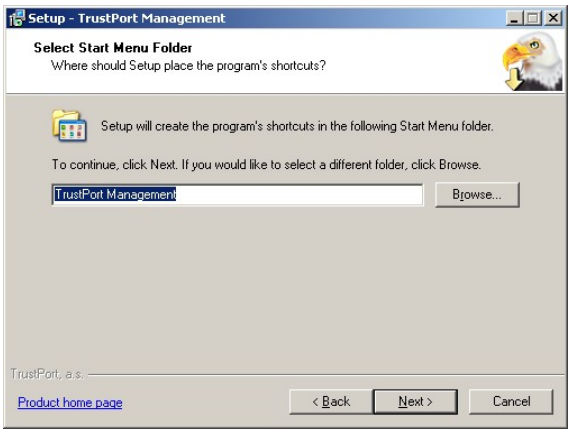


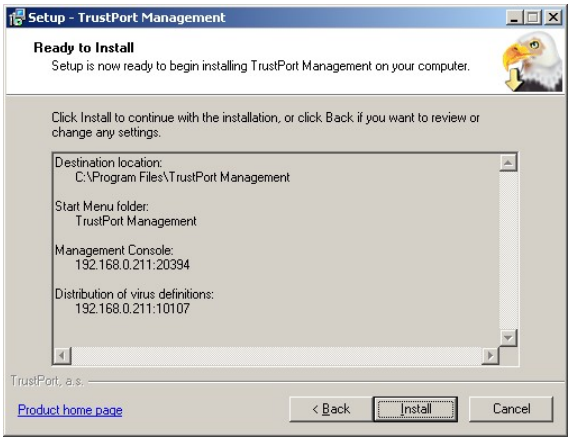
You can define the ports here for communication of the Clients with the Management Console and the pattern file updates.



You can define a password for the Administrator and the Auditor in the next step.

What you miss, however, is the Active Directory support. In the case of larger networks, as an Admin, you do not wish to grapple with a separate user admin for every product used.





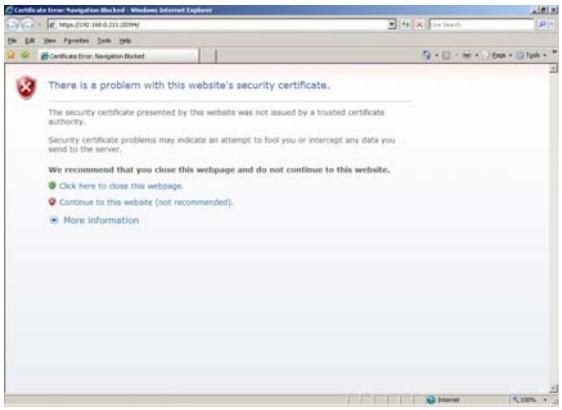
Finally, you have a summary before you can begin with the installation.

At the end of the installation, the system asks you whether you would like to download the latest virus pattern updates right away.

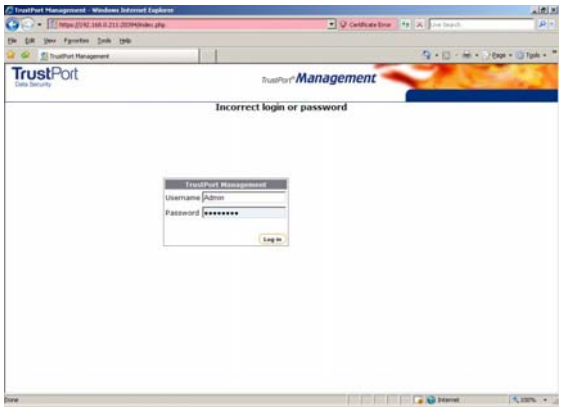
We find this small function very convenient, since you can immediately work with the latest pattern updates. You need

not first configure the central Administration with the help of the update settings.

The update procedure runs in the background if you confirm the query in the affirmative. It would have been nice if a small info notification had been displayed in the taskbar.

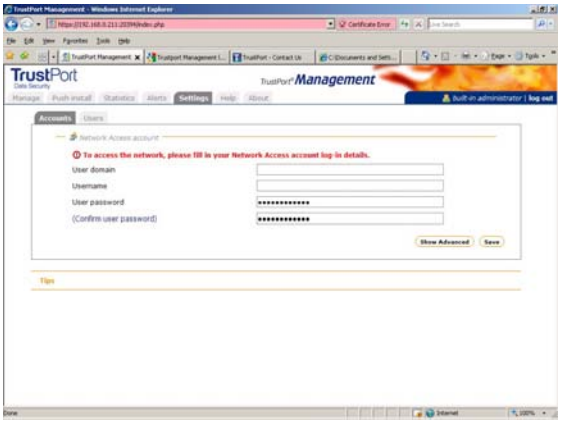


We are aware of the certificate warning from a sufficiently large number of other products, which work with a web admin user interface.



You must note when logging in for the first time that the user name for the Admin or the Auditor account is also case-sensitive. You can get quickly exasperated with such a trivial issue, since you are not necessarily accustomed to it.

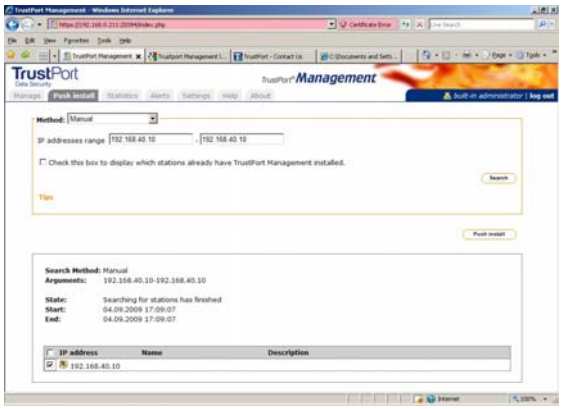
It has been foreseen that there is always one Administrator and many Auditors who are logged in to the system. There is no detailed administration for user privileges. As a result, this product is not necessarily recommended for networks having complex security policies.

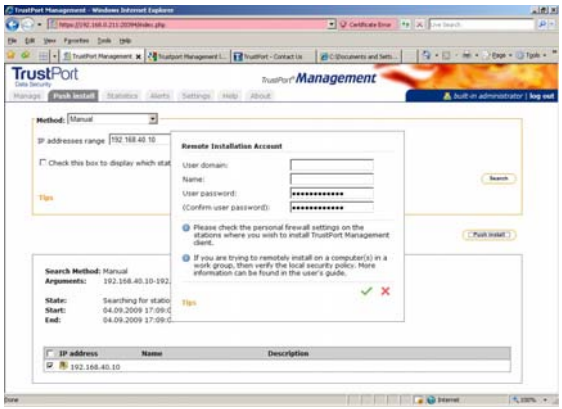


In the next step, the system prompts you for an Admin account, with which network access should be permitted. You can refer to the manual for detailed information regarding the privileges that a user must have in order to be able to execute the push installations and the configuration updates. In this case, we use the domain Administrator account for the sake of simplicity.

In the next step, we invoke the installation wizard for the Client. You can search for the Clients automatically or you can specify the IP range.

In the case of high-security networks, you can have some information regarding the FW configuration ready at hand, so that you can find the Clients.





In the next step, you shall specify the login data for the installation account once again.

Here again, you would have desired to have Active Directory support. In that case, you can obviate the need for specifying the user.

If you have found a Client, you can install the Management Client on the Clients with the help of the "Push Installation" button.

The user cannot detect the installation of the 2.6 MB large Management Client at all and it is executed very quickly.

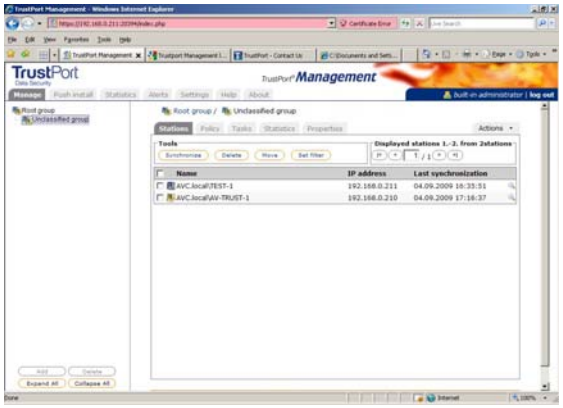
The Management Client can also be distributed with the help of MS AD via GPOs.

TrustPort is no exception here and while the installation on the Client is in progress, apart from very meager status messages, the Admin is kept totally in the dark regarding the progress of the installation.

It is especially in large networks that you can have a very time-consuming debugging effort if 100 out of 1,000 Clients could not be installed for some unknown reason.

It is not clear to us why the users are not provided with the option of a mature and well-designed logging facility or, in fact, the facility of real-time logging. However, as already mentioned, almost all the other AV manufacturers also see it this way.

In the next step, you download the TrustPort Antivirus Business suite in order to begin with the installation of the virus protection via the Management Console.

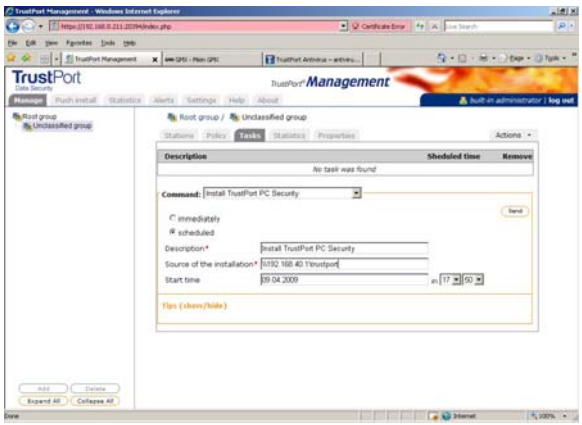


After including your Client and installing the Management Client on the computer, you can see the system appear in the somewhat rudimentary management system provided.

Here too, attention is drawn to the simple design of the filter methods and the views. In the event of a large number of Clients, this would become quite cluttered very quickly.

You can define groups and assign the Clients to their respective groups.

After you have marked your Client, you can go to the "Tasks" tab:



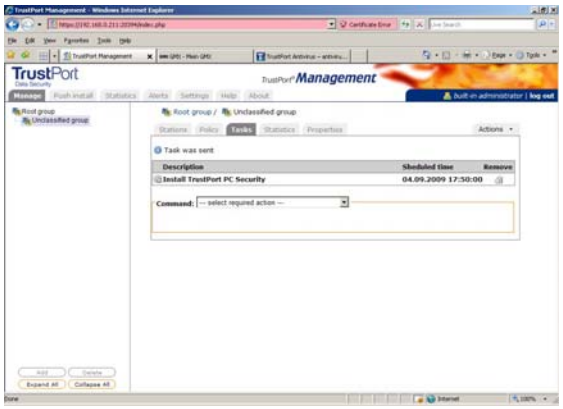
You select the option: "Install TrustPort PC Security" under "Command".

For the push installation of the TrustPort products, it is necessary to create a network share manually, via which the Clients fetch the software.

This should definitely get integrated in the installation Clients!

The user-friendliness has been dispensed with along the way for selecting the path, as a result of which you have to enter the address manually. A browser search should definitely be integrated here.

The installation commences after you have created the installation task successfully. There is no real status information provided.



The Client begins to fetch the latest virus pattern files from the Internet immediately and without posing a query for this purpose. If the TrustPort Antivirus is managed by central administration, it downloads virus signatures directly from superagent (or server). If the server is not found it downloads it from the internet.

Items that are not set in the policy are allowed and can be changed. Items sets by administrator cannot be changed by user. After the installation, only items that set the location for AV engines updates are configured automatically.

Thus, he can also shutdown the Client if he wishes to do so, naturally.

You can install the suite on both a Client Operating System and a Server Operating System.

Summary:

Manufacturer's Website:

The website has been designed elegantly, even if it is not very comprehensive. The site complies with the prevalent Internet standards. Navigating on the site requires that you somewhat get accustomed to it and you need to spend some time to find your way around it.

You can also order out the products directly from the site and you are not diverted to a local reseller.

The site does not have any security zone of its own, with which you can get information regarding the status of the latest threats. It does not even contain a virus lexicon.

The site is merely a visiting card for the company and it has neither on-line scanners nor removal tools.

The Installation Procedure:

The installation of the suite has been kept very rudimentary, because of which it is very simple and you do not need the manual.

The two products tested by us had been named appropriately, because of which you know immediately the installation file with which you need to begin your work.

MS Active Directory Support has not been implemented. Thus, you have your own user administration, which does not permit too many options for the configuration and settings.

It is possible to have many Auditors – but only one Admin – logged in to the Management Console.

Owing to this authorization concept, the TrustPort suite is not suitable for complex security environments.

The system enquires about the first update directly after the installation. Thus, you do not have to click on the console in order to start the first update. This first update runs in the background.

Installing the suite is a breeze and you must note that, when entering the login information, even the username is case-sensitive, since this can lead to problems very quickly because you are not accustomed, by and large, to the fact that even the username is case-sensitive.

Remote installation runs with the bare minimum of settings and executes like a breeze. Manual intervention is necessary with the Clients for the Windows Firewall. Because of the web user interface used by the Administration console, you have no status information whatsoever, regarding the installation on the Clients.

It is not necessary to create the installation packages first.

In general, the options for settings provided by the installation wizard appeared to be very rudimentary. You cannot configure anything beyond the communication ports and the usernames along with their passwords.

The grouping options, which have been kept very simple, are not suitable for larger rollouts.

A very significant minus point of the installation wizard is that you have to create the network share required for the remote installation files manually. This feature should invariably be integrated into the installation wizard!

Installing the server suite loads the server system severely. Memory consumption rises considerably by 400 MB and the server practically comes to a standstill on many occasions during the installation procedure, because the installation program uses high compression method.

When you start the server, it uses a max of 50 MB of memory (which is very nice).

The system carries out a signature update immediately after the installation has been completed.

The Administrator Console:

A web user interface is used as the administration console for the TrustPort suite, which has been designed to be very static and simple.

You can, however, find your way through the few options for settings very quickly and the desired actions can be controlled very comfortably and conveniently.

A summary site, which can give information regarding the status of the system, is not available.

Logging has been kept very simple and you do not have many options to get information with the help of the various menus.

The situation that the immediate tasks do not appear under the "normal" tasks is not very elegant and convenient.

This Administration Console is not even aesthetically appealing. In general, you can say that the entire console would need to be revised, since, in its present form, it is suitable only for very small networks.

AV Clients:

The Client does not differentiate between the Server and the Client Operating Systems.

After installation has been completed, the policy supplied along with the system intervenes, which is suitable only to a limited extent for Server Operating Systems. The Client also enables Internet protection immediately by default and closes ports that have not been assigned. Such a behavior, especially, can lead to very unpleasant consequences on a Server system.

The Client installation runs like a breeze and the user does not need to make any manual intervention.

The operation of the Client has also been kept very simple, owing to which even those users who are not well versed with the system can find their way around with the program very quickly.

A fatal aspect is that the user has complete access to all functions of the tool. The minimum Windows privileges are ade-

quate to administer the Client completely or, in fact, even to disable it. Such a situation is unjustifiable from the security point of view and should be changed.

The message pop-ups are not an eye-sore. The first pop-up to appear after the installation has been completed is an advertisement banner. This situation is probably attributable to the fact that a trial version of the system was used.

Application Areas:

The suite, however, is only suitable for small networks owing to the bare minimum of configuration settings available. The security settings, non-availability of AD support and the Spartan-like user administration disqualify the suite for use in complex corporate environments.

Conclusion:

The TrustPort suite is ideal for small networks. If you are looking for a compact and fast virus scanner having the bare minimum of administration effort, this suite is just the right choice for you.

The suite is not suitable for complex environments having detailed security policies owing to the absence of AD support, rudimentary facilities for user administration, non-availability of central configuration options and settings and the casual administration of privileges.

The Management Console has been provided only with the most important functions but does not leave much room for setting various configurations.

An attractive feature is that it provides monitoring of ports and interfaces on the PC as a standard. Thus, by inserting a USB stick, it immediately asks if the Client should scan the device.

Overall, the TrustPort suite, when it is used in the "correct" environment, is an AV solution that is easy to install and administer.

Pros and Cons:

+ Very simple options for settings
+ Client installation is fast
+ USB and interface monitoring at the Clients

- No summary site in the Admin console
- Moderate user administration
- Authorization settings

Application Areas:

Small Networks (0-50 Users)	Medium Networks (50-500 Users)	Large Networks (500-? Users)
★★★★	★★★	★★

Installation Wizard	★★★
User Navigation	★★★★
Administrator console	★★★
Default Values	★★
MS Active Directory Support	
Database Support	★
Remote Installation	★★★
Website	★★★★
Manual	★★★

Copyright and Disclaimer

This publication is Copyright © 2009 by AV-Comparatives e.V. ®. Any use of the results, etc., in whole or in part, is ONLY permitted with the explicit written approval of the Management Board of AV-Comparatives e.V., prior to their publication. AV-Comparatives e.V. and its appointed representatives carrying out the tests cannot be held liable for any damage or loss, which might occur, as a result of, or in connection with, the use of the information provided in this document. We have taken every possible care to ensure the correctness of the basic data, but no liability can be taken for the correctness of the test results by any representative of AV-Comparatives e.V. We do not give any guarantee for the correctness, completeness, or suitability for a specific purpose of any of the information /content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian non-profit organization.

Please visit our website for more information about AV-Comparatives and the testing methodologies deployed.

AV-Comparatives e.V. (May 2009)

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Recommended Product for							
up to 5 Clients, Server	Avira AntiVir Professional	ESET Smart Security	G Data Antivirus Business	Kaspersky Small Office Security	Sophos Computer Security (Small Business Edition)	Norton Internet Security	TrustPort PC Security
up to 25 Clients and 1 Fileserver	Avira NetWork Bundle	ESET Smart Security Business Edition	G Data Antivirus Business	Kaspersky Business Space Security	Sophos Computer Security (Small Business Edition)	Symantec Endpoint Protection Small Business Edition	TrustPort PC Security with TrustPort Net Gateway
up to 25 Clients and Fileserver and Messaging Server	Avira NetWork Bundle	ESET Smart Security Business Edition and Messaging Bundle	G Data Antivirus Enterprise	Kaspersky Enterprise Space Security	Sophos Security Suite (Small Business Edition)	Symantec Protection Suite Small Business Edition	TrustPort PC Security with TrustPort Net Gateway
more than 25 Clients, more than 1 Fileserver, more than 1 Messaging server	Avira AntiVir Business Bundle	ESET Smart Security Business Edition and ESET Mail Security (or ESET NOD32 Antivirus for MS Exchange)	G Data Antivirus Enterprise	Kaspersky Enterprise Space Security	Sophos Endpoint Security and Data Protection	Symantec Protection Suite Enterprise Edition	TrustPort PC Security with TrustPort Net Gateway
Features Management Server							
What is the maximum number of clients overall?	20000	unlimited	50000	unlimited	unlimited	unlimited	20000
What is the maximum number of clients that can be managed from a single management server under the following conditions: All necessary components (database, repositories, update mechanisms, reporting, etc) are installed on this server and the Clients communicate with the server either continously or at least once per hour	20000	10000	1000	20000	25000	50000	2000
Required minimum hardware (CPU/Mem/Disc)		Hardware needs only to be strong enough to support the OS, and only optionally the Database	Core 2 Duo 2 GB RAM 1,5 GB	Intel Core 2 Duo E8400, 3,00 GHz, 4 GB RAM, HDD SATA 300 GB	Dual/4GB/Raid 0+1	For less than 10000 users we recommend 2 GB and a single processor. For more than 10000 user we recommend at least 4 GB of RAM and a dual processor machine. The disk requirement is mainly influenced by the time that log data is stored on the server and can range from a few GB to several TB.	P4/1GB/0.5-3.0 GB
Does the product provide a mechanism to limit the data transferred over WAN Links when updating clients in remote locations?				●	●	●	
By designating one client as local source for definition updates (Super Agent, Group Update Provider)		●		●		●	●
Does the product provide a mechanism to prevent updates over expensive network connections like UMTS?		configurable	configurable			●	

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Does the product provide a delta update mechanism?	●	●	●	●	●	●	●
Does the product allow customers to use 3rd party tools for virus signature distribution?		no, but signatures can be distributed manually by copying them to the update folder		●	●	●	
Which options does the product provide to ensure that only authorized administrators can administer the product?	Authentification username, password	Password protection, encrypted communication	Adminpassword	Authentification username, password	Password protection, encrypted communication, role-based administration	Authentication / Encryption	Login/Paswd in SSL encrypted pages
Require minimum password length				Depends on Windows Security Policy	●	●	●
Lock administrator account after entering a password multiple times (prevent brute force attack)	●			Depends on Windows Security Policy	●	●	
Log out administrator if idle for a specified time	●			Depends on Windows Security Policy	●	●	●
Client / Server Communication							
Does the client authenticate the server?	●	●	●	●	●	●	
Does the server authenticate the client?	●	●	●	●	●	●	
Is the communication between the client and the server encrypted?	●	●	●	●	●	●	
Does the product support a 'pull' communication mode?	●	●	●	●	●	●	●
Can the communication interval be modified?	●	●	●	●	●	●	●
What is the recommend communication interval?	60 minutes	5 minutes	5 minutes	15 minutes	Real Time	5 minutes	60 minutes
Does the product support a push communication mode?	●	●	●	●	●	●	●
Does the product protect itself from being tampered with by the enduser or malicious software?	●	●	●	●	●	●	
Prevent processes from beeing stopped	●	●	●	●		●	
Prevent files and folders from beeing modified or deleted	●	●	●	●	●	●	
Prevent product registry entries from beeing modified or deleted	●	●		●		●	
Proxy Server							
Can a proxy server be specified?	●	●	●	●	●	●	●
For HTTP	●	●	●	●	●	●	●
For FTP	●			●	●	●	●
Does the product support proxy server authentications?	●	●	●	●	●	●	●

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Master-Slave-Server							
Multiple AV Servers		●	●	●	●	Symantec does not follow a classic master/slave architecture to avoid a single point of failure. Multiple Management Server can perform the same task and replicate content. This has all the benefits of a master/slave architecture (load balancing / local recourses) but avoids a single point of failure	●
Masterserver controls slaveserver in different offices		●	●	●	●	see note above	●
Slaveserver for distributing updates		●	●	●	●	see note above	●
Notes		Slave servers can be nested multiple levels, they each have their own credentials for full access and for read-only access. Policies from upper server can be propagated to lower servers.			Various product versions can be managed withing a few clicks		
Client Installation							
Which client deployment methods does the product support?							
Does the product include a mechanism that allows the administrator to push the software to the clients?	●	●	●		●	●	●
Can the installation of the clients be staggered over time to ensure that the network is not over utilized?	●	●	●	●	●	●	●
Can the administrator see the status of the deployment (i.e. Transfer, Installation in Progress, Installation complete, etc.)?	●	●	●	●	●	●	●
Does the product include a mechanism that allows the end user to download and install the software?	●	●		●	●	●	
Can the admin sent a link which allows the user to download and install the software?		●			●	●	
Does to product support the creation of MSI packages for deployment with 3rd party tools and Active Directory (GPO)?		●		●	●	●	●
Does the product support the creation of single file executable (.exe) installer (i.e. for logon scripts or CD distribution)	●	●	●	●	●	●	●

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Which options can be set for the client installation in the user interface?							
Does the product allow the administrator to define the installation options (i.e. silent, interactive, installation folder, etc) in the user interface?	●	●	●		●	●	●
Which installation types can be defined in the user interface?							
Silent Installation (no user interface is displayed)	●	●	●	●	●	●	●
Unattended installation (the enduser sees the progress of the installation but can not modify the settings)	●	●			●	●	●
Interactive Installation (user choosed the preferences)	●	●			●	●	●
Can the installation folder be specified in the user interface?	●	●		●	●	●	●
Can the administrator define whether the program is added to the Start Menu?		●		●		●	●
Other installation options		Virtually all options of the client can be specified as a parameter of the push installation			Group on bootstrap		Components' selection, additional parameters can be specified via command line
General Capabilities							
Is the system Multi-tenancy capable (host multiple customers on the same infrastructure but separating the data)?			●	●	●	●	
Does the product allow administrators to assign different policies to different groups of computers (regardless of the person logged in)?	●	●	●	●	●	●	●
Does the product allow administrators to assign policies to users (regardless of the computer they use)?	●			●	●	●	
Does the product support static groups (i.e. user or computer are assigned manually to a group or are imported from a third party system)?	●	●	●	●	●	●	●
Does the product support dynamic group assignment based on criteria like IP addresses?	●			●	●	●	
Does the product support hirarchial groups with inheritance?	●		●	●	●	●	●
Location Awareness							
Is the product capable of using different policies, settings and rules depending on the location of the computer?	●		●	●	●	●	

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Which settings/policies can be changed depending on the location?							
Protection technology policies							
Antivirus policies	●		●	●		●	●
Firewall policies			●	●	●	●	●
HIPS & IPS policies				●		●	
Device Control policies				●		●	
Other protection technology policies	Updating		Anti-Spam	Anti-Spam; Updating	Updating		Shredder
Client settings							
User interface configuration	●		●	●		●	●
Communication settings			●	●		●	●
Content update settings	●		●	●	●	●	●
Can the customer define an 'unlimited' number of locations?			●	●		●	
Which criteria can the customer use to define locations?							
Client IP Configuration							
By specifying IP addresses / IP address ranges	●			●	over AD	●	
By specifying Gateway							
By IP address / range	●			●	●	●	
By MAC address	●					●	
The client must have the specified Gateway	●			●	●	●	
The client must not have the specified Gateway	●			●		●	
By specifying DHCP server							
By IP address / range				●		●	
By MAC address						●	
The client must have the specified DHCP server				●		●	
The client must not have the specified DHCP server				●		●	
By specifying the DNS Server Address							
The client must have the specified DNS server				●	●	●	
The client must not have the specified DNS server				●		●	
By specifying DNS suffixes				●	over AD	●	

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
By specifying the type of network connection used or not used by the client (e.g. Ethernet, Wireless, VPN, Dial-up, etc.)	always the adapter that provides the gateway				over AD	●	
By checking whether a client can or can not resolve a DNS host name					over AD	●	
By checking the Registry					over AD	●	
Can multiple criteria be used to define a location?				●	over AD	●	
When are location criteria evaluated?							
Peridocally				●		●	
Immediately when a change in the network configuration takes place (i.e. network adapter enabled / disabled)				●	●	●	
Can the enduser be notified about a location change?						●	
Are location changes logged?				●		●	
Group Import & Synchronisation							
Can computers be imported from a text file?	●	●		●	●	●	
Can computers be imported from Active Directory?	●	●		●	●	●	
Keeping the OU structure defined in Active Directory	●	●		●	●	●	
Using other criteria to assign computers to groups	●	●		●	●	●	
Can changes in Active Directory be synchronized?	●			●	●	●	
Can the synchronisation schedule be defined?				●	●	●	
Can computers be imported from multiple Active Directory server?	●			●	●	●	
Can computers/users be imported from other LDAP server?	●				●	●	
Can computers be imported by a GUI	●	●	●	●	●	●	
Can different actions be defined based on the malware category?			●		●	●	
Scan Location							
Can the administrator exclude/include files and folders from beeing scanned?	●	●	●	●	●	●	●
By file extension	●	●	●	●	●	●	
By predefined lists of extensions provided by the product	●	●		●	●	●	●
By administrator defined lists of extensions	●	●		●	●	●	●
By filenames ("file.txt") regardles of folder or location	●			●		●	●
By filenames & specific folder ("c:\Directory\file.txt")	●	●		●	●	●	●

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
By foldername	●	●		●	●	●	●
Standard Windows folder (i.e. %WINDOWS%, %SYSTEM32%) regardless of the operating system language	●			●		●	●
Does the product provide preconfigured exclusions?	●			●		●	●
Microsoft Exchange							
Exchange 5.5		●				●	
Exchange 2000	●	●		●	●	●	
Exchange 2003	●	●		●	●	●	
Exchange 2007	●	●		●	●	●	
Network shares	●	●	●	●	●	●	●
Is scanning of network shares disabled by default?		●		●	●	●	
Can a user or administrator scan network shares after entering a password?		●		●		●	
System memory / Processes	●		●	●	●	●	●
Does the product scan processes in memory for malware?		●		●	●	●	●
Can the administrator define exceptions (i.e. which processes to igre)?				●		●	
Boot sectors	●	●	●	●	●	●	●
Email Messages							
Does the product scan existing email in the message stores of the following applications?							
Microsoft Outlook	●	●	●	●	●	●	
Microsoft Outlook Express	●	●	●	●	●		
Lotus Notes			●			●	
Thunderbird		●	●		●		
Microsoft Windows Live Mail		●			●		
Microsoft Windows Mail		●					
The Bat!			●	●			
Does the product scan incoming and outgoing emails and attachments in the following protocols?							
SMTP	●	●	●	●	●	●	●
POP3	●	●	●	●	●	●	●
IMAP	●	●	●	●	●		

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Archives							
ZIP/RAR/ARJ & archived installers	●	●	●	●	●	●	●
how deep at on demand (by default)	20	10	100	unlimited	5	10	10
Does the product protect itself against Zip of Death and similar attacks?							
By limiting the recursion depth	●	●		●	●	●	●
By limiting the number of files unpacked					●		
By limiting the size of an unpacked archive		●	●	●	●		
By limiting the processing time for unpacking archives		●		●	●		
Offline files and sparse files							
Does the product allow administrators to define how files with the offline bit set should be handled?							
Skip offline files	●				●	●	
Skip offline and sparse files with a reparse point					●	●	
Scan resident portions of offline and sparse files					●	●	●
Scan all files without forcing demigration						●	●
Scan all files touched within a defined timeframe without forcing demigration					●	●	●
Other locations		Scan floppy drive at shutdown			Removable media	Scan floppy drives at shutdown	Registry, NTFS ADS for files and folders
Does the product provide preconfigured scan locations?	●	●		●	●	●	●
OnDemand Scans							
Can the administrator define when scans should take place?	●	●	●	●	●	●	●
Can the system impact vs. scan speed be defined?	●	●	●	●		●	●
Can the administrator specify which Scan Locations should be included / excluded?	●	●	●	●	●	●	●
OnAccess Scan							
Can the administrator define when a scan is triggered?	●	●		●	●	●	●
Can the administrator specify which Scan Locations should be included / excluded?		●	●	●	●	●	exclude only
Files / Directories		●	●	●	●	●	●
Log							
Which information is logged?							
The Date and time the infection was detected	●	●	●	●	●	●	●

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
The name of the infection and the original location where the infection was found (incl. file name)	●	●	●	●	●	●	●
The malware category (i.e. Virus, Worm, etc)	●	●		●	●	●	
The computer on which the infection was found	●	●	●	●	●	●	●
The user who was logged on at the time the infection was detected	●	●		●	●	●	
The action and current status of the infection (i.e. cleaned, deleted, quarantined, still infected)	●	●	●	●	●	●	●
The current location of the infected file (i.e. local quarantine)	●	●	●	●		●	●
The scan that detected the infection (i.e. OnAccess, Manual, Start-up, etc)	●	●	●	●		●	●
Enduser Interaction							
Let the enduser choose the action	●	●		●	●		●
Notify the enduser							
By displaying a pop up or balloon	●	●	●	●	●	●	●
Can the notifications be customized?	●				●	●	●
By adding a warning to an infected email body or subject (email)	●	●	●	●	●	●	●
By replacing an infected attachment			●	●		●	●
Can the notification can be customized?						●	●
Run a script or application after detection	●			●			
Can a second or alternative action be defined (i.e. if the first action fails)?	●	●	●	●	●	●	●
Which file specific actions can the product perform?							
Clean		●		●	●	●	
Can the product create a backup of the file before attempting to clean it?	●	●		●		●	●
Quarantine on the local system	●	●	●	●	●	●	●
Quarantine in a central location (i.e. management server, quarantine server, etc)		●	●	●	●	●	
Delete		●		●	●	●	●
Deny Access (for OnAccess Scans)		●		●	●	●	●
Which processes specific actions can the product perform							
Terminate the process	●	●		●	●	●	●
Stop the service		●			●	●	●

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Registry Access Rules							
Does the product allow to monitor and prevent access to registry keys and values?				●	●	●	
Does the product allow to define/exclude for which processes (application and services) a registry access rule applies?				●	●	●	
File and Folder Access Rules							
Does the product allow to monitor and prevent access to specific files and folders?					●	●	
Does the product allow to define/exclude for which process a file/folder access rule applies?					●	●	
Which selection criteria does the product provide to specify files and folders?							
By Name					●	●	
By Filenames ("file.txt") regardles of folder or location					●	●	
By Filenames & Specific Folder ("c:\Directory\file.txt")						●	
By Filename and Windows Folder(i.e. #System32#\hosts")						●	
Using wildcards (i.e. *,?)						●	
Using regular expressions						●	
Limit by Location (i.e local drive, CD, USB Stick)		only if mounted as a removable drive			●	●	
Any Local Hard Drive		only if mounted as a removable drive					
Any CD/DVD Drive		only if mounted as a removable drive			●		
Any Network Drive					●		
Any removable media		only if mounted as a removable drive					
Process Access Rules							
Does the product allow to monitor and prevent launching processes?					●	●	
Does the product allow to monitor and prevent terminating processes?						●	
Does the product allow to define/exclude for which processes a process access rule applies?					●	●	
Does the product provide selection criteria to specify processes, e.g. by name?						●	
Process Definition							

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
How can processes (i.e. applications & services) be specified that are allowed/disallowed to perform actions (i.e. modify files, read registry keys, load dlls)?							
By file fingerprint / hash						●	
By filenames & specific folder ("c:\Directory\application.exe")					●	●	
Using wildcards (i.e. *,?)						●	
Limit by location (i.e local drive, CD, USB Stick)					●	●	
Other					By user authorisation and by Behavioral Genotype-based whitelisting identities produced by SophosLabs		
HIPS Actions							
Which actions can be taken when a rule is triggered?		Block		Block	Block, report only, terminate	Block, allow, report, terminate	
Allow Access to the resourse		●		●	●	●	
Block access to the resource		●		●	●	●	
Terminate the process trying to access the resource				●		●	
Can the end user be notified when a rule is triggered?		●		●	●	●	
Can a log entry be created when a rule is triggered?		●		●	●	●	
Conditions							
Which conditions can be checked using the user interface (without using scripts)							
Conditions for files and folder: How can files be specified?							
By filenames ("file.txt") regardles of folder or location	●				●	●	
By filenames & specific folder ("c:\Directory\file.txt")	●	●			●	●	
By filename and windows Folder(i.e. #System32#\hosts")	●					●	
By referencing a value in the registry					●	●	
Which conditions can be specified for file existance							
File exists / does not exist					●	●	
File has specified hash / file fingerprint						●	
File version					●		

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Directory exists					●		
Which conditions can be specified for file (application) versions?							
File version is equal / not equal to specified version					●	●	
File version is higher / lower to specified version					●	●	
Conditions for registry keys and values							
A specified registry key or registry value exists / does not exist					●	●	
Conditions for numeric (DWORD) registry values?							
Is equal / not equal to specified number					●	●	
Is greater / less than specified number					●	●	
Conditions for text (String) registry values?							
Is case sensitive equal / not equal to specified text						●	
Is case in-sensitive equal / not equal to specified text					●	●	
Contains / does not contain specified text (case sensitive)						●	
Contains / does not contain specified text (case in-sensitive)					●	●	
Conditions for binary registry values?							
Is equal to specified value					●	●	
Contains specified value					●	●	
Conditions for processes							
Process or service is running / not running					●	●	
Conditions relating to the operating system							
Type of operating system					●	●	
Language of operating system						●	
Service pack level of the operating system						●	
Is equal / not equal to specified value					●	●	
Is higher / lower than specified value					●	●	
How can conditions be combined?							
If .. Then .., Else						●	
Logical (AND, OR)					●	●	
Can the checks interact with the enduser?							

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Notify enduser (i.e. that an operation will take some time to complete, e.g. by an assesment %)					●	●	
Query enduser						●	
Does to product provide preconfigured conditions?							
Preconfigured Antivirus Check	●	●		●	●	●	
Preconfigured Firewall Check		●		●	●	●	
Preconfigured Patch Management Check		●		●	●	●	
Other					AntiSpyware	Security Best Practice Template	
Remediation							
Does the product provide remediation capabilities?					●	●	
Which remediation action can be defined in the user interface (without resorting to scripts)?							
Registry remediation						●	
File remediation							
Delete files / folders						●	
Download files					●	●	
Process remediation							
Run application in user / system security context					●	●	
Start service in user security context					●	●	
Start service in system security context		●			●	●	
Software Remediation							
Download software and patches					●	●	
Install / uninstall software and patches in user / system security context						●	
Enduser interaction							
Inform user		●			●	●	
Query user		●				●	
Enforcement							
Can the product prevent that a client failing the client health check connects to a network?		●			●	●	
Which enforcement frameworks does the product support?							
Microsoft Network Admission Control						●	

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Cisco Network Access Control		●			●	●	
Symantec Network Access Control						●	
Other					DHCP, 802.1X, VPN	DHCP, 802.1x, VPN, Host Based, Peer, Gateway	
Does the product have inbuild enforcement capabilities?							
Host Based Enforcement / Self Enforcement (i.e. leveraging a desktop firewall to prevent network connections)					●	●	
Other		OPSWAT				Peer to Peer Enforcement	
Behaviour detection							
Behavior detection		●		●	●	●	
Is this technology enabled by default?		●		●	●	●	
General capabilities							
Is the firewall stateful for TCP and UDP connections?		●	●	●	●	●	●
Can the firewall analyze VPN traffic		●		●		●	
Firewall Rules							
Does the product come with default policies?							
For workstations		●	●	●	●	●	●
For server		●					●
Which criteria can be used when defining rules?							
Application							
By filenames ("application.exe")			●	●	●	●	●
By filenames & Specific Folder ("c:\Directory\application.exe")		●				●	●
By File Fingerprint / Hash					●	●	●
By Process					●		
Network adapter type							
Ethernet			●	●		●	●
Wireless			●	●		●	●
VPN			●	●		●	
Dial-up			●	●		●	●
Direction							

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Local / Remote		●		●	●	●	●
Source / Destination		●		●	●	●	●
Remote Host							
By IP address / IP range		●	●	●	●	●	●
By MAC address						●	
By DNS Name					●	●	●
By DNS Domain		●			●	●	●
By Technology Type (incl. RDC, VPN, SSH/SCP, Terminal Services and Citrix)					●	●	
Protocol							
TCP/UDP/ICMP		●	●	●	●	●	●
Raw Ethernet		●			Ability to control network traffic below the IP layer like EAP or PPP and legacy protocols like IPX and Apple Talk	●	
Other			IGMP, GGP, GUP;IDP, GRE		PPTP	Just about any protocol from Apple Talk over IPX, PPTP to X25	
Which Actions can be taken when a firewall rule is triggered?							
Allow/Block traffic		●	●	●	●	●	●
Ask the enduser		●	●	●	●	●	●
Notify enduser when traffic is blocked		●		●	●	●	●
Log							
Log the incident		●	●	●	●	●	●
Include packet data in log		●				●	
Enduser Interaction							
Can endusers be allowed to create firewall rules?		●		●	●	●	●
Can the administrator define rules that can not be overridden by enduser rules?		●	●	●	●	●	●
Can the administrator define rules that can be overridden by enduser rules?		●		●	●	●	
Can the enduser be allowed to disable the firewall?		●		●	●		●
Can the firewall automatically be enabled after a defined time?				●		●	
Can the number of times an enduser can disable the firewall between reboots be limited?						●	

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Can the enduser easily block all network traffic?		●				●	●
Can the enduser be allowed to see the network traffic in real time?		●	●	●		●	●
Firewall Logs							
Which logs are provided?		Critical warnings, Errors, Warnings, Informative records and/or Diagstic records. For troubleshooting, all blocked connections can be logged.		Network attacks, Banned hosts, Application activity, Packet filtering	Allowed in last 10 mins, Allowed today, Blocked 10min/today, Processes, System log	Firewall Log (logs the incidents) and Packet Log (logs the actual packets transmitted)	All critical tices are logged, Rules with specific flag are logged
Can the firewall rules be exported and imported?		●	●	●	●	●	●
Client Management							
Client User Interface							
Can the administrator limit or control configuration changes by the enduser?	●	●	●	●	●	●	●
Can different policies be applied for different computers?	●	●	●	●	●	●	●
Depending on the location of the device (i.e. Office, Hotel, Home, etc)	●			●		●	
Depending on group membership of the computer	●	●	●	●		●	●
Depending on group membership of the user (i.e. administrator vs. normal user)				●	●	●	
Actions							
Which actions can be inititated in administration console?							
Update signatures	●	●	●	●	●	●	●
Reboot computer				●		●	●
Scan computer	●	●	●	●	●	●	●
Enable OnAccess Scan	●	●	●	●	●	●	●
Enable/Disable Firewall		●	●	●	●	●	●
Other		Change all aspects of configuration, including handing off a client to another server	mail scan on/off		Comply with policy, Clean up, Initiate scans, Acknowledge alerts, Protect (install/reinstall) etc.		
On which systems can the actions be initiated?							
A single computer	●	●	●	●	●	●	●
A group of computers	●	●	●	●	●	●	●

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
All computers matching certain criteria (i.e identified by logs or reports)		●		●	●	●	
Other					Automatically deploy to discovered machines in AD		
Can the status of the actions be tracked?	●	●		●	●	●	
Is there a webbased console?		No. The console is windows based and can run from any computer on the network and access the server from there. The console software is portable and can run from a thumbdrive.			●	●	●
Administrator Management							
Rights							
Does the product support multiple administrators?	●	One per server (master server, slave servers)	●	●	●	●	there can be logged more auditors, but only one administrator can be logged at the same time
Does the product support different access levels for administrators?	●	●		●	●	●	●
Access Control							
Can accesss for administrators be limited?	●	●		●	●	●	
Authentication mechanism							
Can administrators be authenticated using an integrated authentication mechanism (i.e. username / password)?	●		●		●	●	●
Does the product enforce minimum password lenghts?					●	●	●
Does the product enforce maximum password age?					●	●	
Can administrators be authenticated using Active Directory?				●	●	●	
Can administrators be authenticated using RSA Secure ID technology?						●	
Other			Domain User Account		SEC uses AD, NAC and Encryption use separate authentication		
Account Security							
Does the product lock an administrator account when a wrong password is provided multiple times (prevent brute force attacks) and can it be unlocked automatically after some time or manually by the administrator?					●	●	

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Does the product log an administrator out after beeing idle for some time?	●			●		●	●
Administrator Auditing							
Does the product keep an audit log?				●	●	●	●
Which changes are logged?							
Log-in / Log-out				●	Over AD	●	●
Changes to policies				●		●	
Changes to system settings				●		●	
Changes to groups				●		●	
Change to administrative accounts				●		●	
Which information is logged							
Time of change				●		●	●
The administrator who performed the action				●		●	●
The action that was performed				●		●	●
Device Control							
Does the product allow administrators to limit the use of external devices (USB sticks, printers, etc)?		●			●	●	
Can the product identify devices by							
Device ID		●			●	●	
Manufacturer ID / Unique ID					●	●	
Can you exclude e.g. printer USB Ports from being scanned	●	●				●	
Can you lock							
DVD		●			●	●	
Floppy		●			●	●	
external media		●			●	●	
USB		●			●	●	
other		All ports and all removable media can be locked, but it's possible to add exceptions for any individual ports or media			WiFi, IR, Bluetooth, Modems, Firewire, SATA, PCMCIA, Bluray, CD, Unencrypted/Encrypted USB devices, Network bridging	Anything that registers as a device with Windows. Bluetooth, IR, Printers. The product tries to prevent administrators from disabling devices that are absolutely necessary like the primary disk drive.	

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
(N)IPS							
Can the product prevent computers from receiving netbios traffic originating from a different subnet?		●			●	●	
Prevent MAC spoofing by allowing incoming and outgoing ARP traffic only if ARP request was made to that specific host						●	
Detect portscans		●		●	●	●	
Does the product detect and prevent denial of service attacks?		●		●		●	
Does the product provide a signature based network intrusion prevention systems?	●	●		●	●	●	
Can a customer create custom IPS signatures?						●	
Does the product include attack facing signatures?	●	●		●	●	●	
Does the product include vulnerability facing signatures?	●	●		●	●	●	
Which actions can be performed?							
Traffic can be allowed / blocked / dropped		●		●	●	●	
Incident can be logged	●	●		●	●	●	
Failover							
What if the AV Server (local) hangsup							
automat. switching to a second local server	●	●	●	●	●	●	●
updates from vendor-server instead of local server	●	●	●	●	●	●	●
other				any other network shared folder		Update from server in other location	if no superagent is accessible in same subnet, primary server will be used and if this server is not accessible then vendor server will be used as a fallback
Quarantine							
Quarantine Folder							
Is there a centralized quarantine-folder			●	●	●	●	
Is there a quarantine-folder on the client	●	●	●	●	●	●	●
can adminstrators specify the location of the quarantine folder anywhere	●	●			●		
rechecking quarantine							

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
after an signature update, is the quarantine folder checked?		●		●		●	
automatically		●		●		●	
manual	●			●	●	●	
undo av-action if false positive is detected		●		●	●	●	

Messaging							
Exchange	Exchange	Exchange	Exchange	Exchange	Exchange	Exchange	Exchange
Feature overview Messaging							
Modules and functional areas		Special module for Exchange. Full integration with MS Exchange, scans the whole Exchange store. Managable from the central management server. Supports 64-bit Exchange.	GateWay Solution		Complete defense against spam, phishing, malware and data leakage. An upcoming add-on will enable email encryption.	In addition to Microsoft Exchange Protection the Suite includes email gateway protection with the Brightmail Gateway appliance or virtual appliance. Antivirus, Antispyware, Antiphishing, Antispam, Content Filtering, Data Loss Prevention	
Malware detection							
Recursive scan of all e-mails and file attachments in real time, event-and time-controlled.	●	●	●	●	●	●	
Information Store scan on every server.	●	●		●		●	
Support of automatic virus pattern updates.	●	●	●	●	●	●	
Scanning of e-mail message text and attachments.	●	●	●	●	●	●	
Detecting file attachments by means of clear, non-manipulable file patterns or by file type, detects and blocks even manipulated files	●	●	●		●	●	
Definition of file limitations by a combination of file name, file extension and file size.	●	●		only by file extension and by time	●	●	
Application of the restrictions on file archives such as zip, rar	●	●	●		●	●	
Automatic detection of new mailboxes		●	●	●	●	●	

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Examination of encrypted e-mails for viruses in combination with Crypt			●		Optionally possible through integration with email encryption server or as part of upcoming on-box encryption capability.		
Scanning of existing mailboxes	●	●		●		●	
AntiSpam							
scan according to the company's policies on prohibited, not desirable or confidential content	●				●	●	
Blocking unwanted e-mail senders (spam senders, mailing lists, etc.) as well as to unwanted recipients (e.g. competitors)	●		●		●	●	
Analysis of images on undesirable content (e.g. pornography)	●				●		
Using current spam pattern for the fast detection of new spammer tricks	●		●		●	●	
User-Specific Management of White- and blacklists on the server solely for effective blocking unwanted e-mails	●		●		●	●	
Definition of transmitter / receiver channels on a dedicated e-mail communications						●	
Freely editable exclusion list for addresses and content in subject and message text	●				●	●	
Flexible notifications of blocked e-mails (directly or schedule) to administration or transmitter/receiver email	●		●		●	●	
User-specific access to e-mails in the quarantine	●				●	●	
Centralized quarantine management	●				●	●	
Formation of company-specific e-mail categories	●				●	●	
Automatic classification of e-mails to one or more categories	●				●	●	
Response Management through defined classifications, for example, the customer support automatic forwarding of e-mails to qualified employees	●				●	●	
Document protection: Following categories may, for example, all outgoing e-mails on company-related content should be examined					●	●	
A content audit of e-mail attachments is also possible					●	●	
if the same mail is deliverd several times, would it be blocked as spam			●				

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Feature overview Messaging	General Windows	General Windows	General Windows	General Windows	General Windows	General Windows	General Windows
Modules and functional areas		Integration with most Windows mail servers is possible through the command line scanner	GateWay Solution		Complete defense against spam, phishing, malware, and data leakage.		TrustPort Internet GateWay serves as the SMTP AV, AS, Antiphising, etc. Protection installed either on the Mail server or on the dedicated server.
Malware detection							
Recursive scan of all e-mails and file attachments in real time, event-and time-controlled		●	●	●	●		●
Information Store scan on every server				●	●		
Support of automatic virus pattern updates	●	●	●	●	●		●
Scanning of e-mail message text and attachments	●	●	●	●	●		●
Detecting file attachments by means of clear, non-manipulable file patterns or by file type, detects and blocks even manipulated files			●	●	●		
Definition of file limitations by a combination of file name, file extension and file size				●	●		●
Application of the restrictions on file archives such as zip, rar			●	●	●		●
Automatic detection of new mailboxes			●		●		
Examination of encrypted e-mails for viruses in combination with Crypt			●	●			
Scanning of existing mailboxes		●			●		
AntiSpam							
scan according to the company's policies on prohibited, not desirable or confidential content					●		●
Blocking unwanted e-mail senders (spam senders, mailing lists, etc.) as well as to unwanted recipients (e.g. competitors)			●		●		●
Analysis of images on undesirable content (eg pornography)					●		●
Using current spam pattern for the fast detection of new spammer tricks.			●		●		●
User-Specific Management of White-and blacklists on the server solely for effective blocking unwanted e-mails.			●				●
Freely editable exclusion list for addresses and content in subject and message text					●		●
Flexible notifications of blocked e-mails (directly or schedule) to administration or transmitter/receiver email			●		●		●

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
User-specific access to e-mails in the quarantine					●		●
Centralized quarantine management					●		●
Formation of company-specific e-mail categories					●		
Automatic classification of e-mails to one or more categories					●		
Response Management through defined classifications, for example, the customer support automatic forwarding of e-mails to qualified employees					●		
Document protection: Following categories may, for example, all outgoing e-mails on company-related content should be examined					●		
A content audit of e-mail attachments is also possible					●		
if the same mail is deliverd several times, would it be blocked as spam			●				
Feature overview Messaging	General Linux	General Linux	General Linux	General Linux	General Linux	General Linux	General Linux
Modules and functional areas		Special product for Linux mail servers. Includes Antispam, web administration interface. Managable from the central management console.	GateWay Solution		Complete defense against spam, phishing, malware, and data leakage.		
Malware detection							
Recursive scan of all e-mails and file attachments in real time, event-and time-controlled.		●	●	●	●		
Information Store scan on every server.		●		●			
Support of automatic virus pattern updates.		●	●	●	●		
Scanning of e-mail message text and attachments.		●	●	●	●		
Detecting file attachments by means of clear, non-manipulable file patterns ("fingerprints") or by file type, detects and blocks even manipulated files.		●	●		●		
Definition of file limitations by a combination of file name, file extension and file size.		●		●	●		
Application of the restrictions on file archives such as zip, rar.		●	●	●	●		
Automatic detection of new mailboxes.		●	●		●		
Examination of encrypted e-mails for viruses in combination with Crypt			●		Optionally possible through integration with email encryption server.		
Scanning of existing mailboxes		●		●			

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
AntiSpam							
scan according to the company's policies on prohibited, not desirable or confidential content					●		
Blocking unwanted e-mail senders (spam senders, mailing lists, etc.) as well as to unwanted recipients (e.g. competitors)		YES to blocking unwanted senders, NO to blocking unwanted recipients	●	●	●		
Analysis of images on undesirable content (eg pornography)				●	●		
Using current spam pattern for the fast detection of new spammer tricks		●	●	●	●		
User-Specific Management of White- and blacklists on the server solely for effective blocking unwanted e-mails		●	●	●	●		
Freely editable exclusion list for addresses and content in subject and message text		●			●		
Flexible notifications of blocked e-mails (directly or schedule) to administration or transmitter/receiver email			●	●	●		
User-specific access to e-mails in the quarantine.					●		
Centralized quarantine management					●		
Formation of company-specific e-mail categories					●		
Automatic classification of e-mails to one or more categories					●		
Response Management through defined classifications, for example, the customer support automatic forwarding of e-mails to qualified employees					●		
Document protection: Following categories may, for example, all outgoing e-mails on company-related content should be examined					●		
A content audit of e-mail attachments is also possible				●	●		
if the same mail is deliverd several times, would it be blocked as spam			●				

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Language:							
In which languages are your corporate products available?	For SLA customers	Management Server and Console (English, Japanese), Client (Bulgarian, Simplified and Traditional Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, French Canadian, English, German, Hungarian, Italian, Japanese, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Slovenian, Spanish, Swedish, Turkish, Ukrainian)	German, English, French, Italian, Spanish	KAV for Windows Workstations & KAV for Windows Servers- 12 languages (English, Russian, Estonian, French, German, Italian, Japanese, Polish, Portuguese, Portuguese (Brazil), Spanish, Turkish).Kaspersky Administration Kit - 7 languages (English, Russian, French, German, Spanish, Polish, Italian).	English, Spanish, French, Italian, German, Chinese, Japanese	English, German, Brazilian, Czech,French, Italien, Japanese, Korean, Polish, Russian, Traditional Chinese, Simplified Chinese, Spanish	Server/Gateway: English, Czech. Client: English, German, Spanish, Italian, Czech
In which languages are your (help) manuals available?	Server (SMC): German, English. Client (AV9): german, english, spanish, russian, italian	English, Bulgarian, Simplified and Traditional Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, French Canadian, English, German, Hungarian, Italian, Japanese, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Slovenian, Spanish, Swedish, Turkish, Ukrainian	German, English, French, Italian, Spanish	KAV for Windows Workstations & KAV for Windows Servers - 10 languages (English, Russian, French, German, Italian, Japanese, Polish, Portuguese, Portuguese (Brazil), Spanish). Kaspersky Administration Kit - 7 languages (English, Russian, French, German, Italian, Japanese, Spanish).	English, Spanish, French, Italian, German, Chinese, Japanese	English, German, Brazilian, Czech,French, Italien, Japanese, Korean, Polish, Russian, Traditional Chinese, Simplified Chinese, Spanish	Server/Gateway: English, Czech. Client: English, German, Spanish, Czech
Support							
24/7/365 phone support	for SLA customers	for SLA customers	no, only weekdays, 8-20 hrs CET	for SLA customers	yes, Free to all	for SLA customers	for SLA customers
Dial Rates	Depends on location	Toll Free Numbers are available in most countries	Depends on location	Depends on location	Depends on location	Toll Free Numbers are available in most countries	Depends on location

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Supported Support Languages	German, English	ESET has four regional offices (US and Canada, Slovakia, Czech Republic, Argentina), all of the offices provide technical support in their local languages. In addition ESET has exclusive distributors in 50 countries and value added resellers in over 100 additional countries. Support in those countries is provided in local language by the local distributor, who in turn receives support directly from ESET.	German, English, French, Italian, Spanish	Local in countries of presence and English	English, Spanish, French, Italian, German, Japanese	English, French. German, Italian. Spanish, Japanese, Cantonese, Mandarin, Korean - While English is the primary language used to provide technical telephone support, best efforts are made to provide local language support in non-English speaking regions	E-Mail: English, German, Spanish, Czech, Slovak Phone: English, Czech, Slovak
Remote Desktop Control for support	●	●	●	●	●	●	●
Support per Forum	●	●		●		●	
Support over Email	●	●	●	●	●	●	●
Guaranteed E-Mail response within		Guaranteed response for Premium 24/7/365 business support is 1 hour.				Support cases will be acknowledged within 15 minutes.	3 hrs (weekdays, 8-16 hrs CET)
On-Site service?	●	●	●	●	●	●	only in Czech Republic

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Service							
Managed by Vendor, this means, can the whole management process be done as a service by the vendor?		Possible by reseller	Possible by reseller	●		●	
Why should users choose your product and not another?	Best detection, fast product, 20 years of experience and continuity, Proven protection	ESET offers the best performance and requires the least resources on workstation. ESET is also the unmatched leader in proactive protection - ESET holds the most AV-Comparatives ADVANCED+ awards in Proactive/Retrospective tests. Centralized management is easy, effective and fits organizations of all sizes.	G Data security solutions offer the highest malware-detection by using the G Data DoubleScan technology. The G Data concept of easy administration saves time and money - long term trainigs are not any more necessary.	Our product was designed with large enterprise corporate networks in mind. We do have multiple enterprise customers with 50K+ who have chosen our system due to its flexibility and manageability. We do support server hierarchy with unlimited nesting. The same is also applicable to user groups. We strongly believe that in large corporate networks the only way to eliminate chaos is through properly designed structure of user groups.	Sophos and Sophos products are geared towards supporting businesses. Offer Anti-virus, anti-spyware, data loss prevention, device control, application control, network access control and encryption through a single product. Simple-to-use products with low total cost of ownership. Central management of Windows, Mac, Linux, Unix clients. Broadest platform support. Direct support 24/7/365 included in licence. Upgrades and updates are included within the licence price (no extra charges). Protection provided by global, integrated SophosLabs 24/7/365	Provide end-to-end protection of laptops, desktops, servers, mobile devices, and messaging infrastructure with more than traditional antivirus and antispyware. Proactive technologies such as TruScan™ Proactive Threat Scan provide protection against unseen threats (i.e., zero-day threats), and do not rely on a signature. The industry-leading antispam technology catches more than 97% of spam with less than one in a million false positives. Extend protection to include desktop/laptop backup and recovery. Easily restore data or systems and protect against new threats through automated, event-driven backups. Rely on our trusted research and over 25 years of experience. Ensure your business is protected with one of the largest security research networks in the world, and the world leader in endpoint security, messaging security, data loss prevention and system recovery.	TrustPort products excel in many security areas including excellent antivirus technology based on several scanning engines, reliable disposal of threats such as classic viruses, macroviruses, trojans, and worms. The anti-spam technology includes a wide range of detection methods and efficiently eliminates junk mail. TrustPort solutions also include strong data encryption technologies, and enable working with digital certificates. Most of the features can be centrally administrated by TrustPort Management.

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Pricing							
Szenario A: 5 clients, server, outlook as mailclient							
recommended product	Avira AntiVir Professional	ESET Smart Security	G Data AntiVirus MultiUser	Kaspersky Small Office Security	Sophos Computer Security (Small Business Edition)	Norton Internet Security 5 user pack	TrustPort PC Security
1 year Euro	175	119	74	167	243	80	95
3 years Euro	350	235	195	350	485	N/A	199
1 year USD	245	165	N/A	233	250	110	133
3 years USD	490	330	N/A	490	500	N/A	278
Szenario B SMB: 1 SBS 2003 Server, 25 Clients							
recommended product	Avira NetWork Bundle	ESET Smart Security Client/Server/Messaging Bundle	G Data AntiVirus Enterprise	Kaspersky Business Space Security	Sophos Security Suite (Small Business Edition)	Symantec Protection Suite Small Business Edition	TrustPort PC Security with TrustPort Net Gateway
1 year plan EURO	1015	735	1342	715	1381	2109	1030
3 year plan EURO	2030	1544	2309	1609	2762	N/A	2162
1 year plan USD	1421	931	N/A	1002	1606	1862	1230
3 year plan USD	2842	1862	N/A	2254	3212	N/A	2582
Szenario C: 1 Fileserver, 1 Exchangeserver, 200 Clients							
recommended product	Avira AntiVir Business Bundle	ESET Smart Security Business Edition + ESET NOD32 Antivirus for Microsoft Exchange	G Data AntiVirus Enterprise	Kaspersky Enterprise Space Security	Endpoint Security and Data Protection	Symantec Protection Suite Enterprise Edition	TrustPort PC Security with TrustPort Net Gateway
1 year plan EURO	8600	5236	8.060	5165	7550	14421	5408
3 year plan EURO	17200	11000	13.744	11621	15100	N/A	11367
1 year plan USD	12050	7389	N/A	5234	8600	14705	6496
3 year plan USD	24100	14779	N/A	16275	17200	N/A	13638

Featurelist	AVIRA	ESET	G Data	Kaspersky	Sophos	Symantec	Trustport
Szenario D, 2 Fileserver, 1 Exchangeserver, 1000 Clients							
recommended product	Avira AntiVir Business Bundle	ESET Smart Security Business Edition + ESET NOD32 Antivirus for Microsoft Exchange	G Data AntiVirus Enterprise	Kaspersky Enterprise Space Security	Endpoint Security and Data Protection	Symantec Protection Suite Enterprise Edition	TrustPort PC Security with TrustPort Net Gateway
1 year plan EURO	27090	17060	23951	18642	25250	56770	16800
3 year plan EURO	54180	35820	39839	41953	50500	N/A	35280
1 year plan USD	37900	23940	N/A	26106	28750	60982	20160
3 year plan USD	75800	47880	N/A	58752	57500	N/A	42304
Szenario E: 10 Fileserver, 10 Exchangeserver, 10000 Clients							
recommended product	Avira AntiVir Business Bundle	ESET Smart Security Business Edition + ESET NOD32 Antivirus for Microsoft Exchange	G Data AntiVirus Enterprise	Kaspersky Enterprise Space Security	Endpoint Security and Data Protection	Symantec Protection Suite Enterprise Edition	TrustPort PC Security with TrustPort Net Gateway
1 year plan EURO	163400	131600	190380	135069	refused to give a price	334234	102400
3 year plan EURO	326800	276600	316030	303806	refused to give a price	N/A	209040
1 year plan USD	228825	182179	N/A	189150	refused to give a price	373874	122400
3 year plan USD	457650	364358	N/A	425450	refused to give a price	N/A	249840
All prices are MSRP (Manufactured Suggested Retail Price). Actual retail prices may differ considerably esp. for Szenarios D and E, as for large projects many factors and savings may apply. Please contact the vendors for actual project prices. The here listed prices are just a rough estimation.				All figures are provided from European price-list.			TrustPort Management is provided free of charge to all customers who bought TrustPort Antivirus and/or TrustPort PC Security products.

We do not take any responsability for the info provided in the above table, as this information was mainly provided by the vendors.
The information is based on the products which were available at the time of the review.

	AVIRA	AVIRA	AVIRA	ESET	ESET	ESET	G Data	G Data	G Data	Kaspersky	Kaspersky	Kaspersky	Sophos	Sophos	Sophos	Symantec	Symantec	Symantec	TrustPort	TrustPort	TrustPort
Supported Operating Systems	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client	Management Server	Management Console	Protection Client
Apple																					
Mac OS																		not all features supported		●	
Mac OS X															●			not all features supported		●	
Mac OS X Server															●			not all features supported			
iPhone OS																					
iPod OS																					
Windows 2000																					
Professional	●	●	●	●	●	●			●	●	●	●	●	●	●	●	●	●	●	●	●
Server	●	●		●	●	●			●	●	●	●	●	●	●	●	●	●	●	●	●
Advanced Server	●			●	●	●			●	●	●	●	●	●	●	●	●	●	●	●	●
Advanced Server 64 Bit Intel	●			●	●	●							●	●	●	●	●	●	●	●	●
Advanced Server 64 Bit Itanium													●	●	●					●	
Data Center Server	●			Untested	Untested	Untested							●	●	●	●	●	●	●	●	●
Data Center Server 64 Bit Intel	●			Untested	Untested	Untested							●	●	●	●	●	●	●	●	●
Data Center Server 64 Bit Itanium													●	●	●					●	
Windows XP																					
Home		●	●	●	●	●	●	●	●		●	●	●	●	●			●		●	●
Professional		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Professional 64 Bit Intel		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Media Center				●	●	●	●	●	●				●	●	●			●	●	●	●
Media Center 2004				●	●	●	●	●	●				●	●	●			●	●	●	●
Media Center 2005				●	●	●	●	●	●				●	●	●			●	●	●	●
Tablet PC Edition				●	●	●	●	●	●				●	●	●			●	●	●	●
Embedded				●	●	●	●	●	●				●	●	●			not all features supported			
Windows Server 2003																					
Standard	●			●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Enterprise 32 Bit	●			●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Enterprise 64 Bit	●			●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Data Center 32 Bit	●			Untested	Untested	Untested	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Data Center 64 Bit	●			Untested	Untested	Untested	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Small Business Server	●			●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Cluster Server				Untested	Untested	Untested	●	●	●				●	●	●	●	●	●			
Storage Server				●	●	●	●	●	●				●	●	●	●	●	●			
Web Edition				●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			
Windows Vista																					
Home Basic 32 Bit		●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●
Home Basic 64 Bit		●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●
Home Premium 32 Bit		●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●
Home Premium 64 Bit		●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●
Business 32 Bit		●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●
Business 64 Bit		●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●
Ultimate 32 Bit		●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●
Ultimate 64 Bit		●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●
Windows Server 2008																					
Standard 32 Bit	●			●	●	●	●	●	●	●	●	only KAV for WSEE	●	●	●	●	●	●	●	●	●
Standard 32 Bit - Core Installation	●			command line only	command line only	command line only	●	●	●			only KAV for WSEE	●	●	●			●	●	●	●
Standard 64 Bit	●			●	●	●	●	●	●	●	●	only KAV for WSEE	●	●	●	●	●	●	●	●	●
Standard 64 Bit - Core Installation	●			command line only	command line only	command line only	●	●	●			only KAV for WSEE	●	●	●	●	●	●	●	●	●
Enterprise 32 Bit	●			●	●	●	●	●	●	●	●	only KAV for WSEE	●	●	●	●	●	●	●	●	●
Enterprise 64 Bit	●			●	●	●	●	●	●	●	●	only KAV for WSEE	●	●	●	●	●	●	●	●	●
Data Center 32 Bit	●			Untested	Untested	Untested	●	●	●	Untested	Untested	only KAV for WSEE	●	●	●	●	●	●	●	●	●
Data Center 64 Bit	●			Untested	Untested	Untested	●	●	●	Untested	Untested	only KAV for WSEE	●	●	●	●	●	●	●	●	●
Web Edition 32 Bit	●			●	●	●	●	●	●	Untested	Untested	only KAV for WSEE	●	●	●	●	●	●		●	
Web Edition 64 Bit	●			●	●	●	●	●	●	Untested	Untested	only KAV for WSEE	●	●	●	●	●	●		●	
Foundation 32 Bit				●	●	●	●	●	●				●	●	●			●		●	
Foundation 64 Bit				●	●	●	●	●	●				●	●	●			●		●	
HPC 32 Bit				Untested	Untested	Untested	●	●	●				●	●	●					●	
HPC 64 Bit				Untested	Untested	Untested	●	●	●				●	●	●					●	

	AVIRA	AVIRA	AVIRA	ESET	ESET	ESET	G Data	G Data	G Data	Kaspersky	Kaspersky	Kaspersky	Sophos	Sophos	Sophos	Symantec	Symantec	Symantec	TrustPort	TrustPort	TrustPort
Windows Mobile																					
Windows Mobile 5.0 Smart Phone						●						●			●			●			
Windows Mobile 5.0 PocketPC						●						●			●			●			
Windows Mobile 6.0 Standard						●						●			●			●			
Windows Mobile 6.0 Professional						●						●			●			●			
Windows Mobile 6.1 Standard						●						●			●			●			
Windows Mobile 6.1 Professional						●						●			●			●			
Windows 7 (unofficially)				●	●	●				●	●				●			●		●	●
Works for Citrix				Untested	●	●	●	●	●			only KAV for WSEE			●			●			
Symbian																					
OS 9.0												KMS EE						not all features supported			
OS 9.1												KMS EE						not all features supported			
OS 9.3												KMS EE						not all features supported			
Series 60												●						not all features supported			
Linux																					
Redhat																					
Redhat Enterprise Linux 3.x 32 Bit						●					●	●			●			●			
Redhat Enterprise Linux 3.x 64 Bit						●									●			●			
Redhat Enterprise Linux 4.x 32 Bit						●					●	●			●			●			
Redhat Enterprise Linux 4.x 64 Bit						●									●			●			
Redhat Enterprise Linux 5.x 32 Bit						●			●		●	●			●			●			
Redhat Enterprise Linux 5.x 64 Bit						●			●		●	●			●			●			
SUSE																					
SUSE Linux Enterprise Desktop 9.x 32 Bit						●									●			●			
SUSE Linux Enterprise Server 9.x 32 Bit						●					●	●			●			●			
SUSE Linux Enterprise Desktop 9.x 64 Bit						●					●				●			●			
SUSE Linux Enterprise Server 9.x 64 Bit						●					●	●			●			●			
SUSE Linux Enterprise Desktop 10.x 32 Bit						●			●						●			●			
SUSE Linux Enterprise Server 10.x 32 Bit						●			●		●	●			●			●			
SUSE Linux Enterprise Desktop 10.x 64 Bit						●			●						●			●			
SUSE Linux Enterprise Server 10.x 64 Bit						●			●		●	●			●			●			
Novell																					
Open Enterprise Server OES 32 Bit						●					●	●			●			●			
Open Enterprise Server OES 64 Bit						●									●			●			
Open Enterprise Server OES2 32 Bit						●					●	●			●			●			
Open Enterprise Server OES2 64 Bit						●									●			●			
Vmware																					
ESX 2.5.x				●	●	●										In supported guest OS	In supported guest OS	●			
ESX 3.0.x				●	●	●				●	●	●			●	In supported guest OS	In supported guest OS	●			
Other supported OS						Novell NetWare, DOS, Solaris, NetBSD, FreeBSD									FreeBSD, OpenBSD, TurboLinux, AIX, HPUX, Solaris, OpenVMS, Netware, SCO, Ubuntu, NetApp DataONTAP				-	-	-

	AVIRA	AVIRA	AVIRA	ESET	ESET	ESET	G Data	G Data	G Data	Kaspersky	Kaspersky	Kaspersky	Sophos	Sophos	Sophos	Symantec	Symantec	Symantec	TrustPort	TrustPort	TrustPort
Database																					
Does the product require a database	●			YES, built-in and supports some others			●	●		●			●			●			YES, buid-it in (it uses a proprietary solution)		
For how many users/clients is the free database recommended							unlimited	unlimited		5000						5000			2000		
Which database is included (i.e. Microsoft SQL, Sybase, MySQL, etc)				Microsoft Access (jet database) engine			SQL Express	SQL Express		Microsoft SQL			MSDE SQL			Sybase					
Which additional databases are supported																					
Microsoft SQL Server																					
Microsoft SQL Server 2000							●	●		●					●	●					
Microsoft SQL Server 2005				●			●	●		●					●	●					
Microsoft SQL Server 2008										●					●						
Other	MS-Access, any ODBC database			MySQL, Oracle											SQL Express 2005 and 2008				MySQL, SQL lite		
Email Server																					
Microsoft Exchange	●					●	●	●			●	●	●			●					
Domino						●	●	●			●	●	●			●					
Tobit						Untested	●	●													
Linux						●	●	●			●	●	●								
Mac							●	●			●	●									
Novell Netware Server						●						●									
Dell NAS						●															
Kerio						●															

We do not take any responsability for the info provided in the above table, as this information was mainly provided by the vendors.